CA IdentityMinder™

Guia de Implementação

r12.6.1

technologies

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos da CA Technologies:

- CA IdentityMinder ™
- CA SiteMinder®
- CA Directory
- CA User Activity Reporting (CA UAR)
- CA CloudMinder™ Identity Management
- GovernanceMinder (anteriormente chamado CA Role & Compliance Manager)

Entrar em contato com o Suporte técnico

Para assistência técnica online e uma lista completa dos locais, principais horários de atendimento e números de telefone, entre em contato com o Suporte técnico pelo endereço http://www.ca.com/worldwide.

Índice

Capítulo 4: Planejando sua implementação 45

Capítulo 5: Integração com o SiteMinder 67

Capítulo 6: Otimizando o CA IdentityMinder 71

Capítulo 7: Criando um plano de recuperação de falhas 101

Capítulo 1: Gerenciamento de identidades e acesso

Esta seção contém os seguintes tópicos:

Gerenciamento de usuários e acesso ao aplicativo

O típico departamento de TI (Information Technology - tecnologia da informação) enfrenta uma demanda constante para manter contas de usuários. Os administradores de TI deve atender às necessidades urgentes dos usuários, como redefinição de senhas esquecidas, criação de novas contas e fornecimento de suprimentos e equipamento de escritório.

Ao mesmo tempo, eles precisam fornecer aos usuários vários níveis de acesso aos aplicativos. Por exemplo, um gerente de departamento gera ordens de compra e precisa de uma conta em um aplicativo financeiro.

Para atender a demandas cada vez maiores de TI, o CA IdentityMinder fornece um método integrado para gerenciar os usuários e o respectivo acesso aos aplicativos, incluindo:

- Atribuição de privilégios por meio de funções. Especificamente:
  - Funções que permitem que os administradores criem e mantenham contas de usuário
  - Funções que provisionem contas adicionais a usuários existentes (requer provisionamento de suporte)
- Delegação de gerenciamento de usuários e de acesso a aplicativos
- Opções de autoatendimento para que os usuários possam gerenciar suas próprias contas
- Integração de aplicativos de negócios com o CA IdentityMinder
- Opções para personalizar e expandir o CA IdentityMinder

Direitos com base em função

Você concede privilégios aos usuários atribuindo funções. Uma *função* contém tarefas que correspondem às funções do aplicativo no CA IdentityMinder, como a tarefa Criar usuário, às funções em um aplicativo, por exemplo, Criar pedido de compra, ou a modelos de conta que fornecem as contas de usuários, como a conta SAP. Quando uma função é atribuída aos usuários, eles recebem os privilégios correspondentes.

O CA IdentityMinder oferece os seguintes tipos de função:

- Funções de gerenciamento de usuários, que são chamadas de *funções administrativas*.

  As funções administrativas também podem incluir qualquer tarefa que aparecer no console de usuário.

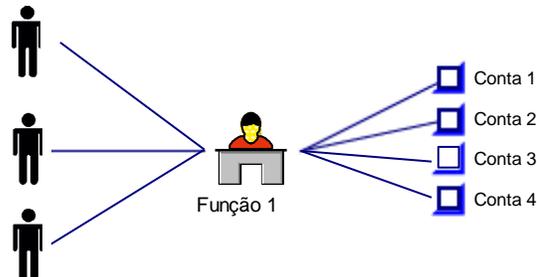
- Funções de atribuição de contas, que são chamadas de *funções de provisionamento*.
- Funções de funcionamento de aplicativo, que são chamadas de *funções de acesso*.

Se você remover uma tarefa ou um modelo de conta de uma função, o usuário não poderá mais executar essa tarefa, usar uma conta do terminal ou usar uma função de aplicativo.

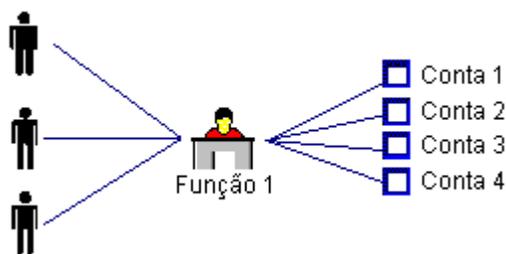
Funções administrativas

As funções administrativas controlam o que um usuário pode fazer no CA IdentityMinder. Um administrador do sistema atribui uma função a um usuário; essa função define um conjunto de tarefas que o usuário pode executar. Os usuários podem executar *tarefas* administrativas em contas de usuário, como alterar uma senha ou atualizar um título da tarefa.

Usuários distintos têm diferentes níveis de acesso a essas tarefas. Por exemplo, uma função de Funcionário pode conter tarefas que oferecem aos usuários a capacidade de modificar seus nomes e endereços, ao passo que a função de Gerente de Recursos Humanos contém tarefas para modificar o cargo e o salário do usuário.

A ilustração a seguir mostra quatro tarefas que são combinadas em uma função administrativa e atribuída a três usuários:

Funções de provisionamento

Para conceder aos usuários acesso às contas em aplicativos adicionais, como um sistema de email, você pode atribuir funções de provisionamento. Funções de provisionamento contém modelos de conta, que definem os atributos que existem em um tipo de conta. Por exemplo, um modelo de conta para uma conta do Exchange define atributos, como o tamanho da caixa de correio. Os modelos de conta também definem como os atributos do usuário do CA IdentityMinder são mapeados para as contas.

A ilustração a seguir mostra quatro contas que são combinadas em uma função de provisionamento e atribuída a três usuários. Cada usuário receberá quatro contas quando você atribuir a função de provisionamento para o usuário.

Funções de acesso

As funções de acesso fornecem uma maneira adicional de fornecer direitos no CA IdentityMinder ou outro aplicativo. Por exemplo, você pode usar as funções de acesso para realizar as seguintes tarefas:

- Fornecer acesso indireto a um atributo de usuário.
- Criar expressões complexas.
- Definir um atributo em um perfil de usuário, que é usado por outro aplicativo para determinar os direitos.

As funções de acesso são semelhantes a políticas de identidade, pois aplicam um conjunto de mudanças nos negócios a um usuário ou grupo de usuários. No entanto, quando você usa uma função de acesso para aplicar mudanças nos negócios, é possível ver para quais usuários as alterações serão aplicadas, exibindo os integrantes da função de acesso.

Na maioria dos casos, as funções de acesso não estão associadas a tarefas.

Observação: quando o CA IdentityMinder se integra com o CA SiteMinder, as funções de acesso também podem fornecer acesso aos aplicativos protegidos pelo CA SiteMinder. Nesse caso, as funções de acesso incluem tarefas de acesso. Para obter mais informações, consulte o capítulo sobre a integração com o SiteMinder no *Guia de Configuração*.

Funções administrativas para gerenciamento de conta de usuário

No CA IdentityMinder, você pode gerenciar objetos de repositório de usuários (usuários, grupos e organizações) por meio de funções administrativas. Também é possível usar funções administrativas para gerenciar as funções e tarefas por meio das quais você gerencia objetos de repositório de usuários. Por exemplo, você pode usar as funções administrativas para modificar os atributos de perfil dos usuários, fornecer aos usuários opções para gerenciar as próprias contas e aprovar tarefas que usem fluxo de trabalho.

Gerenciamento de perfis em nível de atributo

É possível criar funções administrativas para diferentes administradores que precisam ler ou gravar diferentes atributos de perfil. Por exemplo, uma empresa pode ter vários funcionários que executam operações em perfis de usuário, cada um acessando atributos diferentes. A figura a seguir mostra três funções e suas tarefas associadas. Cada função tem acesso diferente aos atributos do perfil.

Tarefas do administrador

Funções de administração

Administrador de TI

UID=Dwalton
Senha=Segredo

Cargo=Admin. de rede

Nome=Dan
Sobrenome= W alton

Endereço=123 Ridge Rd
Cidade=MinhaCidade
Estado=S P

Dias de férias=17

Modificar senha
Exibir UID
Exibir nome
Exibir sobrenome

Administrador de suporte

Exibir UID
Modificar cargo
Modificar nome
Modificar sobrenome
Modificar endereço
Modificar dias de férias

Administrador de RH

Modificar cargo
Exibir nome
Exibir sobrenome
Exibir dias de férias

Gerente de TI

Nesse exemplo, três funções podem gerenciar diferentes atributos para o mesmo usuário, Dan Walton:

- Um administrador de suporte técnico exibe nomes e endereços de usuários e redefine senhas de usuários.
- Um administrador de recursos humanos modifica IDs de usuários, nomes de usuários, endereços, cargos e número de dias de férias.
- Um gerente de TI modifica o cargo dos usuários e exibe o nome e o número de dias de férias.

Seja qual for as funções que você tenha ao efetuar logon no CA IdentityMinder, uma série de guias, denominadas categorias, são exibidas com base na função administrativa atribuída à sua conta do CA IdentityMinder. É possível clicar em uma guia para ver as tarefas que você pode executar nessa categoria, conforme mostrado na figura a seguir:

Logged in as: SuperAdmin
Home
Users
Tasks
Manage Users
Certify User
Create Contractor
Create User
Delete User
Enable/Disable User
Manage Users
Modify User
Request User Modification
Reset User Password
View User
View User Activity
Manage Workitems

As categorias, e as tarefas nessas categorias, que um usuário vê são determinadas de acordo com as funções administrativas do usuário.

Aprovação de tarefas administrativas do fluxo de trabalho

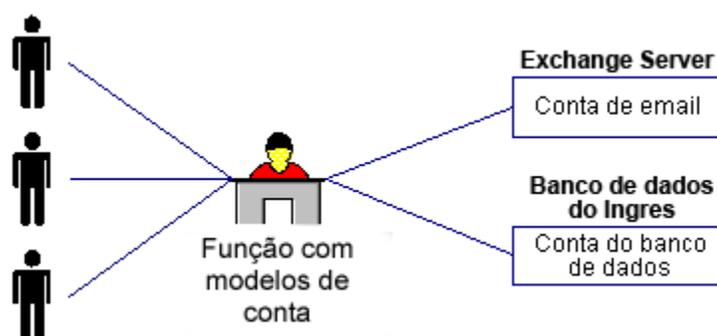
Para ajudar a automatizar os processos de negócios, você pode designar uma tarefa administrativa para gerar um processo de fluxo de trabalho. Um *processo de fluxo de trabalho* automatiza um procedimento bem definido que uma empresa repete com frequência. O CA IdentityMinder inclui o mecanismo de fluxo de trabalho do WorkPoint.

Os processos de fluxo de trabalho são acionados por eventos do CA IdentityMinder que fazem parte de uma tarefa administrativa. Por exemplo, a tarefa Criar usuário inclui eventos chamados CreateUserEvent e AddToGroupEvent. Quando ocorre um evento, o mecanismo de fluxo de trabalho pode:

- Exigir aprovações - um aprovador deve aprovar um evento, como a modificação de um perfil de usuário, antes que o CA IdentityMinder atualize um repositório de usuários. Os aprovadores são administradores que têm a função Aprovador para uma tarefa específica.
- Enviar notificações - o mecanismo de fluxo de trabalho pode notificar os usuários sobre o status de um evento em diferentes etapas de um processo; por exemplo, quando um usuário inicia um evento ou quando um evento é aprovado.
- Gerar listas de tarefas - as listas de tarefas especificam as tarefas que um determinado usuário deve executar. O mecanismo de fluxo de trabalho atualiza as listas de tarefas dos administradores automaticamente.

Para eventos comuns, é possível usar os processos de fluxo de trabalho fornecidos com o CA IdentityMinder. Se preferir, você pode criar processos de fluxo de trabalho personalizados.

Funções de provisionamento para contas adicionais

No CA IdentityMinder, você fornece contas adicionais a usuários usando as funções de provisionamento. As funções de provisionamento contêm modelos de conta, que definem contas existentes em terminais gerenciados, como um servidor de email. Depois que os usuários estiverem no CA IdentityMinder, você poderá atribuir funções de provisionamento a alguns deles. O usuário recebe as contas definidas pelos modelos na função.

Os modelos de conta definem as características da conta. Por exemplo, um modelo de conta para uma conta do Exchange pode definir o tamanho da caixa de correio. Os modelos de conta também definem como os atributos do usuário são mapeados para contas.

Para poder usar funções de provisionamento, é preciso instalar o Servidor de provisionamento com o servidor do CA IdentityMinder. Assim, você poderá criar modelos de conta no Console de usuário.

Gerenciamento de senha

O CA IdentityMinder inclui vários recursos para gerenciar senhas de usuário:

- Políticas de senha - essas políticas gerenciam as senhas do usuário aplicando regras e restrições que controlam a validade, a composição e a utilização da senha.

  Observação: para políticas de senha avançadas, configure a integração com o SiteMinder. Para obter mais informações, consulte o *Guia de Instalação*.

- Gerenciadores de senha - administradores que têm a função Gerenciador de senha podem redefinir uma senha quando um usuário liga para o Suporte técnico.
- Gerenciamento de senha por autoatendimento - o CA IdentityMinder inclui várias tarefas de autoatendimento que permitem que os usuários gerenciem suas próprias senhas. Essas tarefas incluem:
  - Autorregistro - os usuários especificam uma senha quando se registram em um site corporativo.
  - Alterar minha senha - os usuários podem modificar suas senhas sem a ajuda da equipe de TI ou do suporte técnico.
  - Senha esquecida - os usuários podem redefinir ou recuperar uma senha esquecida depois que o CA IdentityMinder verifica sua identidade.
  - ID de usuário esquecida - os usuários podem recuperar uma ID de usuário esquecida depois que o CA IdentityMinder verifica sua identidade.
- Sincronização de senhas (apenas para uso com provisionamento) - as alterações de senha são sincronizadas no CA IdentityMinder e nas contas em sistemas de destino chamados terminais. As novas senhas são verificadas em relação às políticas de senha do CA IdentityMinder.

Opções de autoatendimento para usuários

Para reduzir ainda mais a carga de trabalho de TI, o CA IdentityMinder inclui recursos para registrar novos usuários e fornecer uma senha esquecida. Esses recursos não exigem o envolvimento do administrador. O usuário ganha acesso ao CA IdentityMinder por meio de um *console público*, o que não requer uma conta de logon. Com esse console, um usuário pode se autorregistrar em um site ou solicitar um lembrete para uma senha esquecida.

Para poupar tempo dos administradores de TI, os usuários do CA IdentityMinder podem gerenciar suas próprias contas. Como os usuários têm uma função de autogerenciamento, eles podem:

- Manter informações pessoais
- Alterar a própria senha
- Ingressar em grupos com autoinscrição

Personalização e extensibilidade

Você pode personalizar estes recursos do CA IdentityMinder:

- O diretório do CA IdentityMinder, que descreve uma estrutura de repositório de usuários para o CA IdentityMinder.
- A aparência e a funcionalidade da interface do usuário.
- Telas de entrada do usuário, que determinam os campos e o layout de cada tela de tarefa.
- Validação de entrada de dados do usuário, por meio de implementações Java, JavaScript ou expressão regular.
- Fluxo de trabalho, que define processos automatizados de fluxo de trabalho. Crie ou modifique processos vinculando aprovadores e ações no Designer de processos do WorkPoint.
- Mensagens de email, que informam o status de uma tarefa.
- Envio da tarefa, que pode ser enviada por um aplicativo de terceiros ao TEWS (Task Execution Web Service - serviço web de execução de tarefa) do CA IdentityMinder. O TEWS processa a solicitação de tarefa remota. As solicitações de tarefa remota estão de acordo com os padrões WSDL.

Você pode estender a funcionalidade do CA IdentityMinder usando as seguintes APIs:

- API de atributo lógico — permite exibir um atributo de forma diferente de como ele é fisicamente armazenado em um diretório de usuários.
- API do Manipulador de tarefas de lógica de negócios — permite executar a lógica de negócios personalizada durante operações de transformação ou validação de dados.
- API do fluxo de trabalho — fornece informações a um script personalizado em um processo de fluxo de trabalho. O script avalia as informações e determina o caminho do processo de fluxo de trabalho corretamente.
- API do resolvedor participante - permite que você especifique a lista de participantes que estão autorizados a aprovar uma atividade de fluxo de trabalho.
- API de ouvinte de eventos - permite que você crie um ouvinte de eventos personalizado que escute um grupo de eventos ou evento específico do CA IdentityMinder. Quando o evento ocorre, o ouvinte de evento pode executar lógica de negócios personalizada.
- API de regra de notificação - permite determinar os usuários que devem receber uma notificação por email.
- API de modelo de email - inclui informações específicas de evento em uma notificação por email.

Observação: para obter informações sobre as APIs do CA IdentityMinder, consulte o *Guia de Programação do Java*.

Quando o CA IdentityMinder inclui provisionamento, você também pode estender a funcionalidade de provisionamento da seguinte maneira:

- Conectores personalizados - ative a comunicação entre um Servidor de provisionamento e um sistema do terminal. O código que integra um conector pode incluir um plugin de GUI, plugin de servidor e plugin de agente.

  Um conector dinâmico pode ser gerado pelo Connector Xpress e um conector estático personalizado pode ser desenvolvido em Java ou C++.

  Observação: para obter mais informações, consulte o *Guia do Connector Xpress*.
- Saídas de programa - permite que você faça referência a um código personalizado no fluxo de processo do Servidor de provisionamento.

Observação: para obter mais informações sobre como estender a funcionalidade de provisionamento, consulte o *Guia de Programação de Provisionamento*, que está disponível na mídia Componentes herdados.

Integração do CA RCM

O CA RCM é um produto de gerenciamento do ciclo de vida de identidade, que permite desenvolver, manter e analisar precisamente os modelos de função. Ele também fornece controles centralizados de política de conformidade de identidade e automatiza processos associados ao atendimento de demandas de segurança e conformidade. Usando o CA RCM, você pode executar as seguintes tarefas:

- Verificar se os privilégios de usuário do CA IdentityMinder foram concedidos de acordo com as políticas de conformidade corporativa
- Obter funções sugeridas e verificação de conformidade ao criar ou modificar usuários, funções e contas do CA IdentityMinder
- Compreender quais funções existem em sua organização, estabelecer um modelo de função adequado à sua organização e recriar o modelo de função desejado no CA IdentityMinder
- Analisar e manter esse modelo de função à medida que a empresa evolui

O CA IdentityMinder integra-se ao CA RCM de duas maneiras:

- Conector do CA RCM para o CA IdentityMinder

  Um tipo especial de conector que sincroniza automaticamente os dados do privilégio entre o CA IdentityMinder e o CA RCM. Ao usar esse conector, você pode importar dados do CA IdentityMinder no CA RCM ou exportar dados do CA RCM para o CA IdentityMinder.

- Provisionamento inteligente

  Quando o CA IdentityMinder integra-se ao CA RCM, é possível configurar a funcionalidade adicional que permite o uso de informações de função e conformidade, que estão disponíveis em um modelo de função, de modo a oferecer suporte a operações diárias de gerenciamento de identidades. As alterações feitas no CA IdentityMinder atualizam dinamicamente o modelo de função no CA RCM.

Observação: para obter mais informações sobre a integração do CA RCM ao CA IdentityMinder, consulte o *Guia de Integração do CA IdentityMinder* encontrado na biblioteca do CA RCM.

Integração do CA User Activity Reporting

Desde o CA IdentityMinder r12.6, o CA Enterprise Log Manager é chamado de CA User Activity Reporting (CA UAR).

O CA UAR usa o CA Common Event Grammar (CEG) para mapear eventos que se originam em vários sistemas em um formato padrão e armazena todos os eventos, mesmo aqueles que ainda não foram mapeados, para revisão e análise. Além disso, o CA UAR oferece aos usuários uma solução de grande volume para o gerenciamento e a geração de relatórios de dados coletados, utilizando consultas configuráveis a banco de dados e/ou relatórios para pesquisar vários tipos de informação e eventos.

O CA UAR fornece informações mais amplas e detalhadas sobre sistemas não gerenciados e sistemas fora do alcance e controle do CA IdentityMinder, além de permitir a investigação mais aprofundada de identidades.

A integração ao CA IdentityMinder permite que você exiba relatórios centrados na identidade do CA UAR e/ou consultas dinâmicas no Console de usuário do CA UAR usando o Console de usuário do CA IdentityMinder. No Console de usuário, você pode configurar como relatórios e/ou consultas existentes do CA IdentityMinder/CA UAR são exibidos e modificados durante uma investigação mais aprofundada de uma identidade específica.

Relatórios do CA UAR

Os seguintes Relatórios do CA UAR são fornecidos com as definições de função do CA UAR por padrão:

Tarefa	Chama o relatório
Todos os eventos do sistema por usuário	CA IdentityMinder - Todos os eventos do sistema filtrados pela ID de usuário
Gerenciamento de conta por host	Gerenciamento de conta por host
Criações de conta por conta	Criações de conta por conta
Exclusões de conta por conta	Exclusões de conta por conta
Bloqueios de conta por conta	Bloqueios de conta por conta
Atividade do processo de certificação por host	CA IdentityMinder - Atividade do processo por host
Atividade de modificação da política de senha	CA IdentityMinder - Atividade de modificação de política

Capítulo 2: Atendendo às necessidades de negócios

Esta seção contém os seguintes tópicos:

Processando alterações nos negócios

Você pode automatizar o processamento de determinadas tarefas de gerenciamento de identidades usando políticas de identidade. Uma política de identidade é um conjunto de alterações nos negócios que ocorrem quando um usuário atende a uma determinada condição ou uma regra. É possível usar conjuntos de políticas de identidade para:

- Automatizar determinadas tarefas de gerenciamento de identidade, como a atribuição de funções e associação ao grupo, alocação de recursos ou modificação dos atributos de perfil do usuário.
- Aplicar a segregação de tarefas (na página 26). Por exemplo, você pode criar um conjunto de políticas de identidade que proíbe os integrantes da função de Signatário de cheques de ter a função de Aprovador de cheques, e impedir que qualquer pessoa na empresa preencha um cheque de mais US$ 10.000.
- Aplicar conformidade. Por exemplo, você pode auditar usuários que tenham um determinado cargo e ganhem mais de US $100.000.

  As políticas de identidade que aplicam conformidade são chamadas de *políticas de conformidade*.

As mudanças nos negócios associadas a uma política de identidade incluem:

- A atribuição ou revogação de funções, incluindo funções de provisionamento (quando o CA IdentityMinder inclui provisionamento).
- A atribuição ou revogação de associação de grupo.
- A atualização de atributos de um perfil de usuário.

Por exemplo, uma empresa pode criar uma política de identidade que declara que todos os vice-presidentes pertencem ao grupo Integrante do clube campestre e têm a função de Aprovador de salários. Quando o cargo de um usuário muda para vice-presidente e esse usuário é sincronizado com a política de identidade, o CA IdentityMinder adiciona o usuário ao grupo e função apropriados. Quando um vice-presidente é promovido a CEO, deixa de atender à condição na política de identidade de vice-presidente, portanto, as alterações aplicadas por essa política são revogadas, e novas alterações com base na política do CEO são aplicadas.

As ações de alteração que ocorrem com base em uma política de identidade contêm os eventos que podem ser colocados sob controle do fluxo de trabalho e auditados. No exemplo anterior, a função de Aprovador de salários concede privilégios significativos aos integrantes. Para proteger a função de Aprovador de salários, a empresa pode criar um processo de fluxo de trabalho que exige um conjunto de aprovações antes de atribuir a função e configurar o CA IdentityMinder para auditar a atribuição de função.

Para simplificar o gerenciamento de políticas de identidade, estas são agrupadas em um conjunto de políticas de identidade. Por exemplo, o vice-presidente e o CEO podem fazer parte do conjunto de políticas de identidade de Privilégios executivos.

Cumprindo as políticas de negócios

A conformidade é uma governança corporativa que inclui uma ampla variedade de procedimentos que garantem que uma empresa e seus funcionários estão de acordo com as políticas de negócios. Esses procedimentos de conformidade geralmente envolvem documentar, automatizar e auditorar a alocação de direitos a aplicativos e sistemas.

O CA IdentityMinder inclui os recursos a seguir, que oferecem suporte ao gerenciamento de conformidade:

- **Provisionamento inteligente**

  O Provisionamento inteligente é um conjunto de funcionalidades que simplifica a atribuição de função de provisionamento quando o CA IdentityMinder integra-se ao CA RCM. Essa funcionalidade inclui:

  - Funções de provisionamento sugeridas

    O CA IdentityMinder pode fornecer aos administradores uma lista de funções de provisionamento que podem ser adequadas para serem atribuídas a um usuário. A lista de funções de provisionamento é determinada pelo CA RCM, com base nos critérios inseridos pelo administrador.

    As funções de provisionamento sugeridas ajudam a garantir que os usuários tenham os privilégios corretos e que mantenham um modelo de função da empresa.

- Conformidade e mensagens padrão

  Os administradores do CA IdentityMinder podem validar as alterações propostas em um modelo de funções no CA RCM antes de confirmar as alterações. Validar as alterações antes que elas sejam confirmadas ajuda as empresas a manter o modelo que foi definido para suas operações.

  Os usuários podem validar as alterações propostas nas funções de provisionamento (atribuindo-as ou removendo-as), bem como as alterações nos atributos de usuários.

  O CA IdentityMinder executa dois tipos de validação de política:

  - Conformidade

    As alterações propostas são validadas no modelo de função do CA RCM para verificar se elas violam regras de política de negócios predefinidas e explícitas no CA RCM.

  - Padrão

    As alterações propostas são comparadas ao modelo de função do CA RCM para verificar se elas tornam o motivo da alteração "fora de padrão". O CA IdentityMinder também garante que as alterações não alterem significativamente um padrão estabelecido no modelo de função.

    É possível configurar o CA IdentityMinder para executar essas validações automaticamente quando os usuários executam determinadas tarefas ou permitir que os usuários iniciem a validação manualmente.

Você pode implementar o Provisionamento inteligente em um Ambiente do CA IdentityMinder, uma vez que há um modelo de função estabelecido, com base nos dados do CA IdentityMinder no CA RCM.

Observação: para obter mais informações, consulte o *Guia de Administração*.

- **Políticas de identidade**

  É possível criar uma política de conformidade, um tipo de política de identidade (na página 21), que impede que os usuários tenham determinados privilégios se eles tiverem outros privilégios. Por exemplo, você pode proibir a emissão de verificações por usuários que podem aprovar verificações.

  As políticas de conformidade aplicam uma segregação de tarefas em seu ambiente.

- **Relatórios de conformidade**

  O CA IdentityMinder inclui os exemplos de relatórios que exibem o status de conformidade para os usuários em seu ambiente. Ao usar esses relatórios, você pode ver quais usuários não estão em conformidade com as políticas de negócios.

Relatórios de conformidade

O CA IdentityMinder inclui relatórios de exemplo na tabela a seguir, que podem ser usados para monitorar a conformidade com as políticas de negócios corporativas.

Relatório	Descrição
Integrantes da função	Exibe as funções no banco de dados de relatórios e lista os integrantes dessas funções
Funções	Exibe as seguintes informações para cada função no banco de dados de relatórios: ■ Tarefas associadas à função ■ Políticas de integrante e integrantes da função ■ Políticas de administrador e administradores da função ■ Políticas de proprietário e proprietários da função
Funções de tarefas	Exibe as tarefas no banco de dados de relatórios e as funções às quais estão associadas
Funções de usuários	Exibe os usuários no banco de dados de relatórios e lista as funções de cada usuário
Tendência de contas fora do padrão	Exibe tendências de contas fora do padrão para contas órfãs, contas do sistema e contas de exceção.
Contas não padrão	Exibe todas as contas órfãs, do sistema e de exceção
Contas órfãs	Exibe todas as contas de terminal sem usuário global no Servidor de provisionamento
Políticas	Exibe todas as políticas de identidade

Relatório	Descrição
Perfil de usuário	Exibe as seguintes informações dos usuários: ■ Nome ■ ID do usuário ■ Grupos onde o usuário é integrante ou administrador ■ Funções em que o usuário é integrante, administrador ou proprietário
Contas de terminal	Exibe as contas por terminal (você pode escolher qual terminal exibir)
Administradores da função	Exibe as funções e seus administradores
Proprietários da função	Exibe as funções e seus proprietários
Instantâneos	Exibe todos os instantâneos exportados
Conta de usuário	Exibe uma lista de usuários e suas contas
Direitos do usuário	Exibe funções, grupos e contas do usuário
Status da sincronização da política de usuário	Exibe o status do usuário por política (quais políticas devem ser alocadas, desalocadas ou realocadas)

Observação: para obter mais informações sobre relatórios, consulte o *Guia de Administração*.

Aplicando requisitos de segregação de tarefas

Os requisitos de SOD (Segregation of Duties - segregação de tarefas) impedem os usuários de receberem privilégios que possam resultar em um conflito de interesses ou em fraude. O CA IdentityMinder proporciona os seguintes recursos para oferecer suporte à:

- **Políticas de identidade preventivas**

  Essas políticas, que são executadas antes que uma tarefa seja enviada, permitem que um administrador verifique violações de políticas antes de atribuir privilégios ou alterar atributos do perfil. Se uma violação existir, o administrador pode removê-la antes de enviar a tarefa.

  Por exemplo, uma empresa pode criar uma política de identidade preventiva que proíba que os usuários que tenham a função Gerenciador de usuários também tenham a função Aprovador de usuários. Se um administrador usar a tarefa Modificar usuário para fornecer a um gerenciador de usuários a função de Aprovador de usuários, o CA IdentityMinder exibirá uma mensagem sobre a violação. O administrador pode alterar as atribuições de função para remover a violação antes de enviar a tarefa.

- **Validação de política por meio do Provisionamento inteligente**

  Os administradores do CA IdentityMinder podem validar as alterações propostas para funções de provisionamento e atributos de usuário nas BPRs (Business Policy Rules - regras de política de negócios) no CA RCM antes de confirmar as alterações. As BPRs representam várias restrições em privilégios. Por exemplo, uma BPR pode impedir que os usuários que possuem uma função de departamento de compras, que permite aos integrantes solicitar estoque de prestadores de serviços, de também ter uma função de pagamento de prestadores de serviços. Um administrador do sistema, gerente comercial, auditor ou engenheiro de função cria BPRs no CA RCM.

  Observação: para obter mais informações sobre BPRs, consulte o *Guia do Usuário do CA RCM Sage DNA*.

Observação: para obter mais informações sobre as políticas de identidade preventivas e o Provisionamento inteligente, consulte o *Guia de Administração do CA IdentityMinder*.

Transformando dados no repositório de usuários

Em alguns casos, pode ser conveniente que o CA IdentityMinder transforme dados antes que eles sejam colocados no repositório de usuários. Por exemplo, talvez você queira armazenar informações em um formato diferente do que elas são inseridas, ou queira que as alterações sejam aplicadas quando determinados tipos de informações estiverem presentes.

O CA IdentityMinder inclui os seguintes recursos para transformar dados:

- Políticas de identidade
- Manipuladores de atributos lógicos

Observação: você também pode usar políticas de identidade e manipuladores de atributo lógico para implementar a lógica de negócios personalizada.

Manipuladores de atributos lógicos

Os manipuladores de atributos lógicos são códigos Java personalizados que transformam os valores de atributo de usuário usados nas telas de tarefas do CA IdentityMinder. Usando os manipuladores de atributos lógicos, você pode controlar como um atributo físico é exibido em uma tela de tarefas. Você também pode usar os manipuladores de atributos lógicos para transformar um valor de exibição, como custo, na tela de tarefas, em um ou mais atributos físicos, como preço unitário e quantidade, que são armazenados no repositório de usuários.

Observação: para obter mais informações sobre os manipuladores de atributos lógicos, consulte o *Guia de Programação do Java*.

Aplicando a lógica de negócios personalizada

É possível personalizar o CA IdentityMinder para implementar a lógica de negócios de que sua empresa necessita. O CA IdentityMinder inclui as seguintes opções para implementar a lógica de negócios personalizada:

- Políticas de identidade — você pode usar políticas de identidade para definir um conjunto de mudanças nos negócios que ocorrem quando um usuário atende a uma determinada condição ou regra. Por exemplo, as políticas de identidade podem automatizar determinadas tarefas de gerenciamento de identidades, como atribuir funções, ou aplicar regras de negócios, como impedir que os usuários assinem e aprovem cheques acima de US$ 20.000.

  Observação: para obter mais informações sobre políticas de identidade, consulte o *Guia de Administração*.

- Manipuladores de atributos lógicos — você pode associar esses manipuladores às telas de tarefas do CA IdentityMinder para controlar a exibição e a modificação de valores de atributo.

  Para obter mais informações, consulte o *Guia de Programação do Java*.

- Manipuladores de tarefas de lógica de negócios — permitem executar a lógica de negócios personalizada, como a seguir, durante as operações de validação de dados para uma tarefa do CA IdentityMinder:

  - Aplicando as regras de negócios personalizadas (por exemplo, um administrador não tem permissão para gerenciar mais de cinco grupos).
  - Validando campos da tela de tarefas específicos do cliente (por exemplo, o valor de um campo ID do funcionário deve existir no banco de dados de Recursos Humanos mestre).

  Os manipuladores de tarefas de lógica de negócios podem ser implementados em Java ou JavaScript.

  Observação: para obter mais informações, consulte o *Guia de Programação do Java*.

- Fluxo de trabalho — permite que você crie definições de processo personalizadas, que são associadas a um evento do CA IdentityMinder.

Observação: antes de decidir se implementa a lógica de negócios em um manipulador de tarefas de lógica de negócios ou em um processo de fluxo de trabalho, consulte as seções a seguir:

- Considerações sobre o manipulador de tarefas de lógica de negócios (na página 29)
- Considerações sobre o processo de fluxo de trabalho (na página 29)

Considerações sobre o manipulador de tarefas de lógica de negócios

Os Manipuladores de tarefas de lógica de negócios executam a validação da lógica de negócios durante a fase de processamento síncrono da tarefa, que ocorre antes da geração de eventos. Isso permite que você:

- Execute a validação em nível de tarefa. Por exemplo, você pode adicionar ou remover integrantes de um grupo com base no local de trabalho, que é especificado na tela de perfil do usuário.
- Impeça que uma tarefa seja enviada se a validação falhar.
- Transforme automaticamente todas as informações em uma tela de tarefas para que elas estejam em conformidade com suas políticas de negócios antes do envio da tarefa.

Observação: você não deve implementar as atividades que levam muito tempo para serem concluídas em um Manipulador de tarefas de lógica de negócios. As atividades de execução longa atrasam o envio da tarefa e não são ideais para a fase síncrona onde ocorre a interação do usuário. Em vez disso, use um processo de fluxo de trabalho, que é executado durante a fase assíncrona da tarefa.

Considerações sobre o processo de fluxo de trabalho

Os processos de fluxo de trabalho são chamados durante a fase assíncrona da tarefa e são associados à execução de eventos individuais. Isso permite que você:

- Executar atividades de aprovação com base nos dados de eventos individuais
- Executar atividades de lógica de negócios personalizadas de longa duração

Embora a API do fluxo de trabalho permita que você obtenha dados em nível de tarefa de uma Atividade de fluxo de trabalho, normalmente, você estará operando no contexto desse evento específico no fluxo de trabalho.

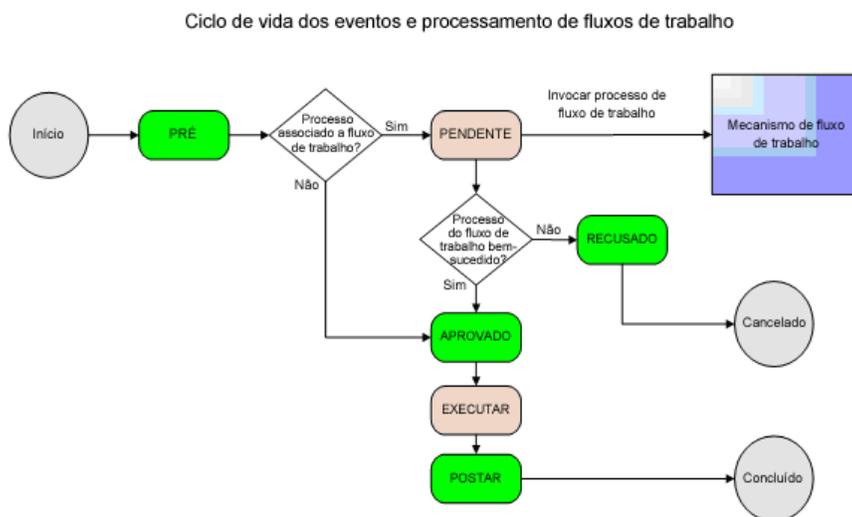
Aprovando alterações nos negócios

O fluxo de trabalho descreve um processo composto por uma ou mais etapas que devem ser executadas para atingir um objetivo de negócios, como a execução de um procedimento de contratação ou a obtenção da pontuação de crédito de um usuário de um sistema externo. Geralmente, uma das etapas em um processo de fluxo de trabalho envolve aprovação ou rejeição da mudança nos negócios.

No CA IdentityMinder, um processo de fluxo de trabalho está associado a um evento, uma ação que ocorre durante o processamento da tarefa. Quando um evento entra no estado Pendente em seu ciclo de vida, o CA IdentityMinder chama qualquer processo do fluxo de trabalho associado e pausa a execução do evento até que o processo seja concluído. O CA IdentityMinder executará ou rejeitará o evento com base nos resultados do processo de fluxo de trabalho.

Esse fluxo é ilustrado no diagrama a seguir:

Ciclo de vida dos eventos e processamento de fluxos de trabalho

Início
PRÉ
Processo associado a fluxo de trabalho?
Sim
Não
PENDENTE
Invocar processo de fluxo de trabalho
Mecanismo de fluxo de trabalho
Processo do fluxo de trabalho bem-sucedido?
Não
RECUSADO
Cancelado
Sim
APROVADO
EXECUTAR
POSTAR
Concluído

O CA IdentityMinder inclui o mecanismo de fluxo de trabalho do InSession WorkPoint para criação e gerenciamento de processos de fluxo de trabalho.

Observação: para obter mais informações, consulte o *Guia de Administração*.

Capítulo 3: Arquitetura do CA IdentityMinder

Esta seção contém os seguintes tópicos:

Componentes do CA IdentityMinder

Uma implementação do CA IdentityMinder pode incluir alguns ou todos os seguintes componentes:

- Servidores
- Repositórios de usuários
- Bancos de dados
- Conectores

Servidores

Uma implementação do CA IdentityMinder inclui um ou mais tipos de servidores, conforme a funcionalidade necessária.

Servidor do CA IdentityMinder (obrigatório)

Executa tarefas no CA IdentityMinder. O aplicativo J2EE CA IdentityMinder inclui o Management Console e Console de usuário.

Servidor de provisionamento do CA IdentityMinder

Gerencia contas nos sistemas do terminal.

Esse servidor será obrigatório se a instalação do CA IdentityMinder oferecer suporte ao provisionamento de conta.

Observação: é necessário ter o Diretório de provisionamento instalado remotamente (ou localmente apenas para um ambiente de demonstração) em um Servidor do CA Directory antes de instalar o Servidor de provisionamento.

Servidor de políticas do SiteMinder

Fornece a autenticação avançada para o CA IdentityMinder e fornece acesso a recursos do SiteMinder, como Serviços de senha e Logon único.

Esse servidor é opcional.

Repositório de usuários e Diretório de provisionamento

Para fornecer opções de gerenciamento de usuários e provisionamento de contas adicionais a esses usuários, o CA IdentityMinder coordena dois repositórios de usuários:

- O *repositório de usuários do CA IdentityMinder*, o repositório de usuários mantidos pelo CA IdentityMinder. Geralmente, esse é um repositório existente que contém as identidades de usuário que uma empresa precisa gerenciar.

  O repositório de usuários pode ser um diretório LDAP ou um banco de dados relacional.

  No Management Console, crie um objeto de Diretório do CA IdentityMinder para se conectar ao repositório de usuários e para descrever os objetos de repositório de usuários que o CA IdentityMinder manterá.

- O *Diretório de provisionamento*, o repositório de usuários mantido pelo Servidor de provisionamento.

  Ele é uma instância do CA Directory e inclui usuários globais, que associa os usuários no Diretório de provisionamento com contas em terminais, como Microsoft Exchange, Active Directory e SAP.

  Somente alguns usuários do CA IdentityMinder têm um usuário global correspondente. Quando um usuário do CA IdentityMinder recebe uma função de provisionamento, o Servidor de provisionamento cria um usuário global.

Diretórios de provisionamento e repositório de usuários separado

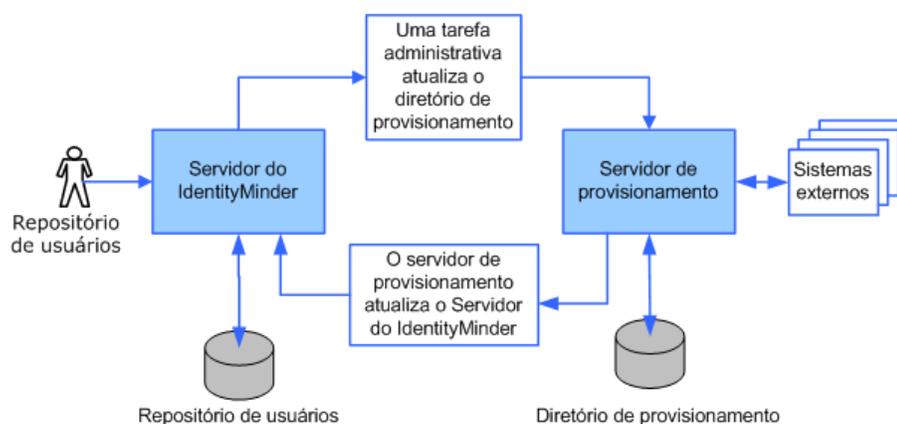
Importante: A CA Technologies recomenda enfaticamente o uso de um repositório de usuários separado e do Diretório de provisionamento para novas implantações.

A figura a seguir mostra um repositório de usuários separado e o Diretório de provisionamento. Nesta figura:

- Um administrador do CA IdentityMinder usa uma tarefa administrativa que edita um usuário no repositório de usuários, que afeta o Diretório de provisionamento.

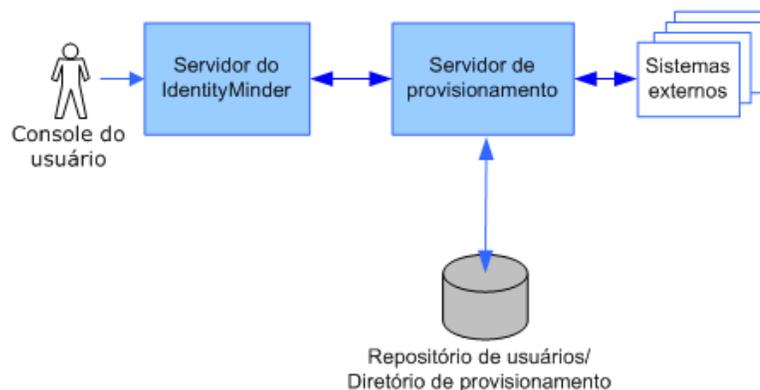
  Essa alteração também pode atualizar um terminal (por exemplo, um servidor de email) que tem um conector com o Servidor de provisionamento.

  Uma alteração feita no Servidor de provisionamento (ou um terminal com um conector para o Servidor de provisionamento) atualiza o repositório de usuários e o Diretório de provisionamento do CA IdentityMinder.

Por exemplo, um terminal, como um aplicativo de Recursos Humanos, pode atualizar os endereços de email dos usuários.

Combinação do repositório de usuários e do Diretório de provisionamento

Se você selecionar uma instância do CA Directory para ambos os repositórios de usuários, o diretório funcionará como um repositório de usuários e Diretório de provisionamento. Os usuários criados no CA IdentityMinder são armazenados nesse diretório, mas você ainda pode modificar esse diretório como um Diretório de provisionamento. Por exemplo, você pode selecionar o atributo de usuário a ser usado no Servidor de provisionamento para um atributo de usuário específico usado pelo CA IdentityMinder.

Importante: A CA Technologies recomenda enfaticamente o uso de um repositório de usuários separado e do Diretório de provisionamento para novas implantações.

A figura a seguir mostra o uso de um diretório para o repositório de usuários e para o Diretório de provisionamento.

Nessa situação, as alterações feitas no repositório de usuários/Diretório de provisionamento podem ser iniciadas pelo CA IdentityMinder, pelo Servidor de provisionamento ou por um terminal.

Observação: quando o CA IdentityMinder usa uma combinação do repositório de usuários e do Diretório de provisionamento, as organizações não são suportados. Se você precisar gerenciar as organizações, use um repositório de usuários separado e o Diretório de provisionamento. Como escolher uma solução de repositório de usuários (na página 52) lista diferenças adicionais entre implementações combinadas e separadas de repositório de usuários/Diretório de provisionamento.

Bancos de dados

O CA IdentityMinder usa origens de dados para se conectar aos bancos de dados que armazenam informações necessárias para oferecer suporte à funcionalidade do CA IdentityMinder. Esses bancos de dados podem residir em uma única instância física de um banco de dados ou em instâncias separadas.

Objeto de banco de dados (obrigatório)

Contém informações de configuração do CA IdentityMinder.

Banco de dados de persistência de tarefas (obrigatório)

Mantém informações sobre as atividades do CA IdentityMinder e seus eventos associados ao longo do tempo. Isso permite que o sistema controle com precisão as atividades do CA IdentityMinder, mesmo que você reinicie o Servidor do CA IdentityMinder.

Banco de dados de arquivamento (obrigatório)

Arquiva dados do Banco de dados de persistência de tarefas.

Banco de dados do fluxo de trabalho

Armazena definições de processo do fluxo de trabalho, tarefas, scripts e outros dados exigidos pelo Mecanismo de fluxo de trabalho.

Banco de dados de auditoria

Fornece um registro histórico de operações que ocorrem em um ambiente do CA IdentityMinder.

Observação: é possível configurar a quantidade e o tipo de informação que o CA IdentityMinder armazena no banco de dados de auditoria. Consulte o *Guia de Configuração* para obter mais informações.

Banco de dados de relatórios

Armazena dados de instantâneo, que reflete o estado atual dos objetos no CA IdentityMinder no momento em que o instantâneo é gerado. Você pode gerar relatórios com essas informações para exibir as relações entre objetos, como usuários e funções.

Ao usar o instalador, o CA IdentityMinder configura uma conexão com um único banco de dados, chamado de Banco de dados do CA IdentityMinder, que contém as tabelas para cada tipo de banco de dados.

Observação: é possível criar um repositório de dados para persistência de tarefa, fluxo de trabalho, auditoria ou relatórios em um banco de dados separado e configurar o CA IdentityMinder para se conectar a ele. Para obter mais informações, consulte o *Guia de Instalação*.

Componentes do conector

Um conector é a interface de software para um terminal. O Servidor de provisionamento usa o conector para se comunicar com o terminal. Ele converte as ações do Servidor de provisionamento em alterações no terminal, como Criar uma conta de email em um terminal do Microsoft Exchange".

Exemplos de terminais são: estação de trabalho UNIX, Windows PC ou um aplicativo, como Microsoft Exchange (para email).

Servidores de conectores

Um servidor de conectores é um componente do Servidor de provisionamento que gerencia conectores. Ele pode ser instalado no sistema do Servidor de provisionamento ou em um sistema remoto.

Um Servidor de conectores funciona com diversos terminais. Por exemplo, se você tiver muitos terminais da estação de trabalho UNIX, você poderá ter um Servidor de conectores que manipule todos os conectores que gerenciam contas UNIX. Outro Servidor de conectores pode manipular todos os conectores que solicitam contas do Windows.

O Servidor de conectores distribuído funciona com vários Servidores de conectores. Ele oferece balanceamento de carga quando um Servidor de conectores está ocupado e alta disponibilidade quando um Servidor de conectores é desativado.

Há dois tipos de servidores de conectores:

- O CA IAM Connector Server (CA IAM CS) gerencia conectores escritos em Java
- O C++ Connector Server (CCS) gerencia conectores escritos em C++

C++ Connector Server

O *C++ Connector Server* é um servidor de conectores que gerencia conectores C++. Ele pode ser instalado no Servidor de provisionamento ou em um sistema remoto. O C++ Connector Server oferece uma estrutura de aplicativo orientada a objetos que simplifica o desenvolvimento de conectores, que são responsáveis pela comunicação entre o C++ Connector Server e o terminal.

CA IAM CS

O CA IAM CS é um componente de servidor que manipula a hospedagem, o roteamento e o gerenciamento de conectores Java. O CA IAM CS fornece uma alternativa Java ao C++ Connector Server. De modo arquitetônico e funcional, ele é semelhante ao C++ Connector Server, exceto pelo fato de que ele apresenta uma API Java em vez de uma API C++, que permite que seus conectores sejam implementados no Java. Além disso, o CA IAM CS é orientado a dados, em vez de orientado ao código, o que permite que mais funcionalidade seja englobada pelo recipiente (ou CA IAM CS), e não pelos conectores em si.

O Servidor de provisionamento controla o provisionamento de usuários e depois delega aos conectores (usando o C++ Connector Server ou o CA IAM CS) para gerenciar contas de terminal e grupos.

Conectores e agentes

Os Conectores do CA IdentityMinder são executados como parte da arquitetura mais ampla do Servidor de provisionamento e se comunicam com os sistemas gerenciados em seu ambiente. Um conector funciona como um gateway para uma tecnologia de sistema do tipo de terminal nativo. Por exemplo, as máquinas que executam o ADS (Serviços do Active Directory) podem ser gerenciadas apenas se o conector do ADS estiver instalado em um Servidor de conectores com o qual o Servidor de provisionamento pode se comunicar. Os conectores gerenciam os objetos que residem nos sistemas. Os objetos gerenciados incluem contas, grupos e, opcionalmente, objetos específicos de tipo de terminal.

Os conectores são instalados no Servidor de conectores e alguns componentes são instalados no Servidor de provisionamento (por exemplo, plugin do Servidor) ou no Gerenciador de provisionamento (plugins de interface de usuário).

Alguns conectores exigem um agente nos sistemas que eles gerenciam para concluir o ciclo de comunicação; nesse caso, eles podem ser instalados usando o Instalador de provisionamento. Os agentes podem ser separados nas categorias a seguir:

Agentes remotos

Instalados em sistemas de terminal gerenciados

Agentes de ambiente

Instalados em sistemas como CA ACF2, CA Top Secret e RACF

Determinados componentes funcionam no Unix e no Windows, incluindo as seguintes opções que se baseiam no C++ Connector Server:

- UNIX (ETC, NIS)
- Controle de acesso (ACC)

  Observação: o conector UNIX ACC pode gerenciar apenas terminais UNIX ACC. O conector Windows ACC é necessário para gerenciar os terminais do Windows ACC, mas também pode gerenciar terminais do UNIX ACC.
- CA-ACF2
- RACF
- CA-Top Secret

Os outros conectores que têm como base o C++ Connector Server podem ser acessados no Servidor de provisionamento Solaris contando com a CSF (Connector Server Framework - estrutura do servidor do conector). A CSF permite um Servidor de provisionamento no Solaris para se comunicar com os conectores em execução no Windows.

Observação: a CSF deve ser executada no Windows para usar esses conectores.

Connector Xpress

O Connector Xpress é o utilitário do CA IdentityMinder para gerenciamento de conectores dinâmicos, mapeamento de conectores dinâmicos para terminais e definição de regras de roteamento para terminais. Você pode usá-lo para configurar conectores dinâmicos de modo a permitir o provisionamento e o gerenciamento de bancos de dados SQL e diretórios LDAP.

O Connector Xpress permite criar e implantar conectores personalizados sem conhecimento técnico, em geral, necessário durante a criação de conectores gerenciados pelo Gerenciador de provisionamento.

Você também pode configurar, editar e remover uma configuração de servidor de conectores (Java e C++) usando o Connector Xpress.

A principal entrada para o Connector Xpress é o esquema nativo de um sistema do terminal. Por exemplo, você pode usar o Connector Xpress para se conectar a um RDBMS e recuperar o esquema do banco de dados SQL. Você pode usar o Connector Xpress para criar mapeamentos das partes do esquema nativo que são relevantes para o gerenciamento e o provisionamento de identidade. Um mapeamento descreve como a camada de provisionamento representa um elemento do esquema nativo.

O Connector Xpress gera metadados que descrevem, para um conector, os mapeamentos de tempo de execução para um sistema de destino.

A saída do Connector Xpress é um documento de metadados gerado quando você conclui seus mapeamentos. Os metadados são um arquivo XML que descreve a estrutura do conector para o CA IAM CS.

Eles descrevem as classes e os atributos do Servidor de provisionamento e como eles são mapeados para o esquema nativo.

Os metadados são usados para criar tipos de terminal dinâmicos em um ou mais Servidores de provisionamento.

Observação: para obter mais informações sobre como usar o Connector Xpress, consulte o *Guia do Conector Xpress*, na *biblioteca do CA IdentityMinder*.

Componentes adicionais

O CA IdentityMinder inclui alguns componentes adicionais, que oferecem suporte à funcionalidade do CA IdentityMinder. Alguns desses componentes são instalados com o CA IdentityMinder e alguns devem ser instalados separadamente.

Fluxo de trabalho do WorkPoint

O mecanismo de fluxo de trabalho do WorkPoint e a Interface de desenho do WorkPoint são instalados automaticamente quando você instala o CA IdentityMinder.

Esses componentes permitem colocar uma tarefa do CA IdentityMinder sob o controle do fluxo de trabalho, bem como modificar as definições existentes do processo de fluxo de trabalho ou criar novas.

Observação: para obter mais informações sobre fluxo de trabalho, consulte o *Guia de Administração*.

Gerenciador de provisionamento

O Gerenciador de provisionamento do CA IdentityMinder gerencia o Servidor de provisionamento por meio de uma interface gráfica. Ela é usada pelas tarefas administrativas, como o gerenciamento das opções do Servidor de provisionamento. Em alguns casos, você também pode usar o Gerenciador de provisionamento para gerenciar determinados atributos de terminal, que você não pode gerenciar no Console de usuário do CA IdentityMinder.

O Gerenciador de provisionamento é instalado como parte das Ferramentas administrativas do CA IdentityMinder.

Observação: esse aplicativo é executado apenas em sistemas Windows.

Para obter mais informações sobre o Gerenciador de provisionamento, consulte o *Guia de Referência de Provisionamento*.

Servidor de relatórios do IAM

O CA IdentityMinder fornece relatórios que você pode usar para monitorar o status de um ambiente do CA IdentityMinder. Para usar os relatórios fornecidos com o CA IdentityMinder, instale o Servidor de relatórios do IAM, incluído com o CA IdentityMinder.

O Servidor de relatórios do IAM é movido pelo Business Objects Enterprise XI. Se você tiver um servidor do Business Objects, não será possível usá-lo no lugar do Servidor de relatórios do IAM para gerar relatórios do CA IdentityMinder.

Observação: para obter instruções de instalação, consulte o *Guia de Instalação*.

Exemplo de instalações do CA IdentityMinder

Com o CA IdentityMinder, você pode controlar as identidades de usuários e do respectivo acesso a aplicativos e contas nos sistemas do terminal. De acordo com a funcionalidade necessária, selecione quais componentes do CA IdentityMinder instalar.

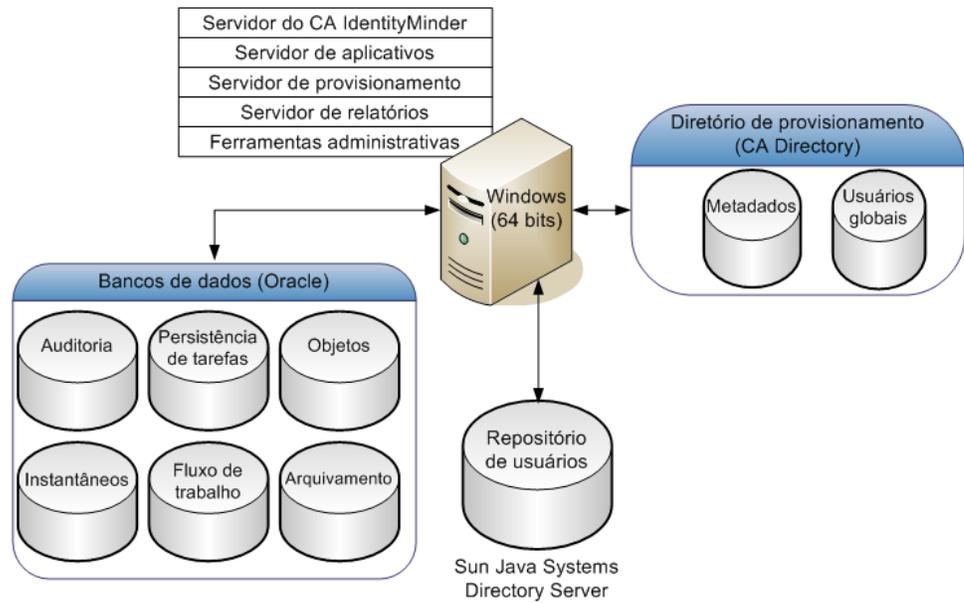
Em todas as instalações do CA IdentityMinder, o Servidor do CA IdentityMinder é instalado em um servidor de aplicativos. Use o Instalador do CA IdentityMinder para instalar os outros componentes necessários.

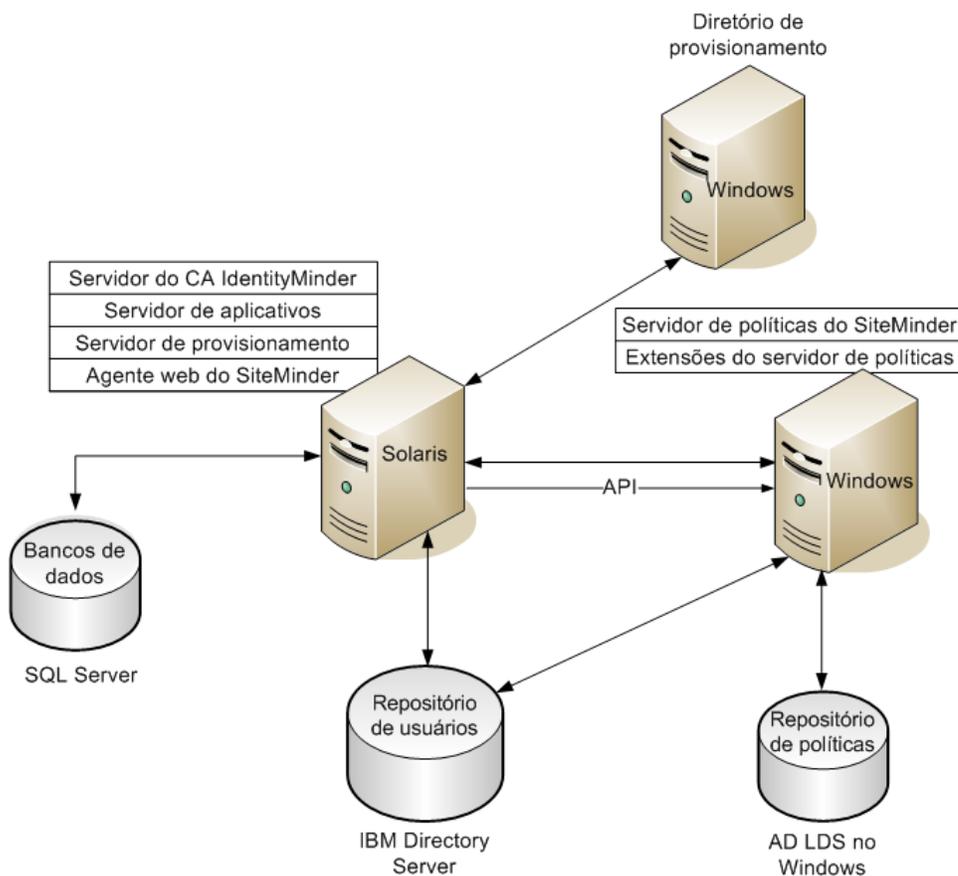
As próximas seções mostram alguns exemplos de implementações do CA IdentityMinder em um alto nível.

Instalação com componentes de provisionamento

O provisionamento do CA IdentityMinder permite criar um Ambiente que se conecta a um Servidor de provisionamento para o provisionamento de contas a vários sistemas do terminal. Você pode atribuir funções de provisionamento a usuários criados no CA IdentityMinder. As funções de provisionamento são funções com modelos de conta que definem contas que os usuários podem receber nos sistemas do terminal. As contas fornecem aos usuários acesso a recursos adicionais, como uma conta de email.

Ao atribuir uma função de provisionamento a um usuário, este recebe as contas definidas pelos modelos de conta na função. Os modelos de conta também definem como os atributos do usuário são mapeados para contas. As contas são criadas em terminais gerenciados definidos pelos modelos de conta.

A figura a seguir é o exemplo de uma instalação do CA IdentityMinder com provisionamento:

Instalação com Servidor de políticas do SiteMinder

Um Servidor de políticas do SiteMinder fornece autenticação e proteção avançadas para seu ambiente do CA IdentityMinder. A figura a seguir é o exemplo de uma instalação do CA IdentityMinder com um Servidor de políticas do SiteMinder:

Uma implementação do CA IdentityMinder que inclui o SiteMinder engloba todos os componentes da instalação básica ou da instalação com provisionamento, além destes componentes adicionais:

Agente web do SiteMinder

Funciona com o Servidor de políticas do SiteMinder para proteger o Console de usuário. O Agente web está instalado no sistema com o Servidor do CA IdentityMinder.

Servidor de políticas do SiteMinder

Fornece autenticação e autorização avançadas para o CA IdentityMinder, e outra funcionalidade, como Serviços de senha e Logon único.

Extensões do Servidor de políticas do SiteMinder

Permite a um Servidor de políticas do SiteMinder oferecer suporte ao CA IdentityMinder. Instale as extensões em cada sistema do Servidor de políticas do SiteMinder na sua implementação do CA IdentityMinder.

Repositório de políticas do SiteMinder

Armazena informações que o SiteMinder precisa para gerenciar o acesso a recursos da web.

Quando o CA IdentityMinder integra-se ao SiteMinder, o repositório de políticas também inclui informações sobre diretórios e ambientes do CA IdentityMinder para que o SiteMinder possa fornecer autenticação avançada.

Observação: os componentes são instalados em diferentes plataformas, como nos exemplos. No entanto, você pode escolher outras plataformas. Os bancos de dados do CA IdentityMinder estão no Microsoft SQL Server e o repositório de usuários está no IBM Directory Server. O Servidor de políticas do SiteMinder está no AD LDS do Windows.

Capítulo 4: Planejando sua implementação

Para planejar uma implementação do CA IdentityMinder, decida como o CA IdentityMinder gerenciará os usuários e qual funcionalidade é necessária para que você atinja seus objetivos de negócios. Veja algumas perguntas que devem ser levadas em consideração:

- Como gerencio usuários?
- Preciso de provisionamento de conta?
- Quais são meus requisitos de negócios personalizados? Devo implementá-los usando o fluxo de trabalho?

Com base nas decisões tomadas, você pode determinar a melhor maneira de implementar o CA IdentityMinder para o seu ambiente.

Esta seção contém os seguintes tópicos:

Decida o que gerenciar

Decidir o que você deseja gerenciar o ajudará a determinar quais componentes instalar. Usando o CA IdentityMinder, você pode gerenciar o seguinte:

- Identidades de usuários
- Acesso a contas em sistemas do terminal

Identidades de usuários

As identidades de usuários representam as pessoas que uma empresa precisa gerenciar, como funcionários, contratados, fornecedores, entre outros.

Para gerenciar as identidades de usuários, é necessário instalar apenas o Servidor do CA IdentityMinder e as Ferramentas administrativas.

Como configurar o suporte ao gerenciamento de usuários

No CA IdentityMinder, você gerencia usuários com funções administrativas, que determinam as tarefas do CA IdentityMinder que os administradores podem executar.

Observação: antes de implementar o gerenciamento de usuários no CA IdentityMinder, é preciso determinar qual funcionalidade é necessária e desenvolver um plano (na página 61) para implementá-la em estágios.

Para configurar o suporte ao gerenciamento de usuários, conclua as seguintes etapas de alto nível:

1. Instale o Servidor e as Ferramentas administrativas do CA IdentityMinder.

   Se precisar provisionar contas a usuários gerenciados, você também precisará instalar o suporte para provisionamento (na página 47).

   Observação: consulte o *Guia de Instalação* para obter instruções.

2. Crie os seguintes itens no Management Console do CA IdentityMinder:

   - **Diretório do CA IdentityMinder**

     Descreve um repositório de usuários para o CA IdentityMinder. Ele inclui os seguintes itens:

     - Um ponteiro para um repositório de usuários, que armazena objetos gerenciados, como usuários, grupos e organizações.
     - Os metadados que descrevem como objetos gerenciados são armazenados no diretório e representados no CA IdentityMinder.

   - **Ambiente do CA IdentityMinder**

     Oferece um namespace de gerenciamento que permite aos administradores do CA IdentityMinder gerenciar objetos, como usuários, grupos e organizações, com um conjunto de funções e tarefas associadas. O ambiente do CA IdentityMinder controla o gerenciamento e a apresentação gráfica de um diretório.

   Para obter mais informações sobre diretórios e ambientes do CA IdentityMinder, consulte o *Guia de Configuração*.

3. Modifique as tarefas e funções administrativas para atender aos seus requisitos de negócios.

   As típicas modificações de função incluem adição ou remoção de tarefas padrão de funções administrativas existentes, ou criação de funções administrativas, que têm como base as funções padrão.

As típicas modificações de tarefa incluem personalização das guias padrão do perfil de usuário para incluir apenas as informações que você deseja gerenciar. (As guias de perfil padrão incluem todos os atributos que são definidos para usuários.)

Para obter informações sobre como modificar funções e tarefas administrativas, consulte o *Guia de Design do Console de Usuário*.

4. Atribua as funções administrativas aos usuários que executarão tarefas de gerenciamento de usuários.

Provisionamento de contas de outros aplicativos

A decisão de implementar o provisionamento depende do tipo de informações que você deve gerenciar. Se você estiver gerenciando um diretório de usuários central e não desejar gerenciar contas de usuário em outros sistemas, o provisionamento não será necessário. Se desejar gerenciar contas de usuário usando uma variedade de sistemas, você deverá implementar o suporte ao provisionamento.

Os recursos de provisionamento são fornecidos por meio do Servidor de provisionamento, que é integrado ao CA IdentityMinder. O Servidor de provisionamento oferece a seguinte funcionalidade para o provisionamento de conta:

- Gerenciamento do terminal
- Sincronização de conta
- Modelos de conta
- Funcionalidade Explorar e correlacionar

Observação: as informações de provisionamento são armazenadas em um Diretório de provisionamento. Se o CA IdentityMinder mantiver usuários em outro tipo de diretório, sua implantação incluirá um repositório de usuários e um diretório de provisionamento do CA IdentityMinder.

Gerenciamento do terminal

Para provisionar contas, defina e gerencie terminais no Console de usuário do CA IdentityMinder. Um *terminal* é um sistema para o qual os usuários precisam de acesso. Exemplos de terminais incluem bancos de dados Oracle, servidores UNIX NIS, servidores Windows e Microsoft Exchange Servers. Use *Modelos de conta* (na página 48) para criar contas e determinar os recursos do usuário em terminais gerenciados.

Observação: também é possível usar o Gerenciador de provisionamento para definir e gerenciar terminais. Embora o uso do Console de usuário para realizar a maioria das tarefas de gerenciamento de terminais seja recomendável, existem algumas tarefas que exigem o Gerenciador de provisionamento, como o gerenciamento de determinados atributos de terminal e o gerenciamento de objetos de terminal, que não sejam contas. Para obter mais informações sobre o Gerenciador de provisionamento, consulte o *Guia de Referência de Provisionamento*.

Sincronização de conta

Você pode sincronizar contas de usuário em vários terminais gerenciados. Quando a sincronização de contas é ativada, uma alteração feita em um perfil de usuário no Servidor de provisionamento é propagada para todos os terminais em que o usuário possui uma conta.

Observação: especifique as configurações de sincronização de contas na guia Perfil de uma tarefa do CA IdentityMinder. Para obter mais informações sobre como configurar a sincronização de contas, consulte o *Guia de Administração*.

Modelos de conta

Os modelos de conta definem como um usuário é representado em um terminal gerenciado. Por exemplo, um modelo para uma conta do Exchange definiria o formato do endereço de email de um usuário como <iniciais><sobrenome>@minha_empresa.com.

Os modelos de conta também determinam os privilégios que um usuário tem em um sistema gerenciado. Por exemplo, além de definir o formato de um endereço de email, um modelo para uma conta do Exchange também pode limitar o tamanho da caixa de correio de um usuário.

Você cria e gerencia modelos de conta no Console de usuário.

Funcionalidade Explorar e correlacionar

Os recursos Explorar e correlacionar simplificam o gerenciamento de terminais detectando e sincronizando alterações em sistemas gerenciados.

O recurso Explorar localiza objetos, incluindo contas, em terminais, e armazena referências para eles no Diretório de provisionamento. Você pode usar o recurso Explorar para detectar todos os objetos novos a serem gerenciados. Por exemplo, se você provisionar contas em um diretório LDAP e novas organizações forem adicionadas nesse diretório, será possível usar o recurso Explorar para apresentar essas novas organizações para uso em modelos de conta.

O recurso Correlacionar associa uma conta em um terminal gerenciado a um usuário global no Diretório de provisionamento. Quando uma alteração é feita na conta por meio do terminal, o recurso Correlacionar pode sincronizar essas alterações com a conta de usuário global.

Observação: para obter mais informações sobre a funcionalidade Explorar e correlacionar, consulte o *Guia de Administração*.

Como configurar o suporte para provisionamento

Após decidir implementar o provisionamento, conclua as seguintes etapas de alto nível.

1. Use o instalador do Servidor do CA IdentityMinder para instalar o Servidor do CA IdentityMinder, o Servidor de provisionamento, a inicialização do Diretório de provisionamento e as Ferramentas administrativas.

   Observação: para obter mais informações sobre como instalar os componentes do CA IdentityMinder, consulte o *Guia de Instalação*.

2. Configure o Gerenciador de provisionamento para se conectar ao Servidor do CA IdentityMinder.

3. Configure o provisionamento no Management Console do CA IdentityMinder:

   a. Ative o provisionamento.

   b. Configure um ambiente para provisionamento executando as etapas a seguir:

      - Importando definições de função personalizadas
      - Configurando um administrador de entrada
      - Conectando o ambiente com o Servidor de provisionamento.

   Observação: para obter mais informações, consulte o *Guia de Configuração*.

4. Crie terminais no Console de usuário.

   Isso permite que o CA IdentityMinder gerencie o terminal.

   Observação: para obter mais informações sobre gerenciamento de terminais, consulte o *Guia de Administração*.

5. Explore e correlacione o terminal.

   Ao explorar um terminal, o CA IdentityMinder localiza os objetos no terminal e armazena as respectivas instâncias no diretório de provisionamento. Esta ação preenche o diretório de provisionamento com contas e outros objetos encontrados no terminal.

   Ao correlacionar contas em um terminal, o CA IdentityMinder as associa a um usuário global no diretório de provisionamento. Você pode escolher se a função de correlação criará algum usuário global que não esteja presente ou se ela associará contas sem nenhum usuário global correspondente ao [usuário padrão] usuário global.

6. Crie e mantenha contas de terminal usando modelos de conta, que contêm os atributos que são usados para criar contas.

7. Associe os modelos de conta a funções de provisionamento.

   Ao atribuir funções de provisionamento aos usuários, o CA IdentityMinder cria contas nos terminais associados desses usuários.

   Observação: para obter informações sobre modelos de contas e funções de provisionamento, consulte o *Guia de Administração*.

Determinar requisitos de auditoria

O CA IdentityMinder inclui recursos de auditoria que permitem monitorar atividades em um ambiente do CA IdentityMinder.

Essas informações são armazenadas em um banco de dados de auditoria. A quantidade e o tipo de informações armazenadas no banco de dados de auditoria são configuráveis.

Você pode exibir dados de auditoria no Console de usuário por meio de uma tarefa chamada Exibir tarefas enviadas. Essa tarefa permite que os administradores procurem e exibam as tarefas que ocorrem no sistema. Os administradores podem exibir informações de tarefa em um nível alto ou exibir detalhes de eventos e tarefas.

Considerações de auditoria do CA IdentityMinder

Os dados de auditoria fornecem um registro histórico de operações que ocorrem em um ambiente do CA IdentityMinder. Para dados de auditoria do CA IdentityMinder, é necessário o seguinte:

- Um banco de dados de auditoria
- Um arquivo de configurações de auditoria

Banco de dados de auditoria

Ao usar o Instalador do CA IdentityMinder, o CA IdentityMinder configura uma conexão com um único banco de dados, chamado Banco de dados do CA IdentityMinder, e cria uma origem de dados para conexão com as tabelas de banco de dados de auditoria.

Observação: o Banco de dados do CA IdentityMinder também inclui dados que estão sendo usados por outras funcionalidades do CA IdentityMinder, incluindo persistência de tarefa, fluxo de trabalho e geração de relatórios. Para fins de escalabilidade, você pode criar uma instância separada de um banco de dados para auditoria.

Observação: para obter mais informações sobre o banco de dados de auditoria, consulte o *Guia de Instalação*.

Configurações de auditoria

É possível definir as configurações de auditoria em um arquivo de configurações de auditoria. Um arquivo de configurações de auditoria determina a quantidade e o tipo de informação que o CA IdentityMinder audita. Você pode definir um arquivo de configurações de auditoria para executar as seguintes ações:

- Ativar a auditoria para um ambiente do CA IdentityMinder.
- Ativar a auditoria de alguns ou todos os eventos do CA IdentityMinder gerados pela tarefas administrativas.
- Registrar informações sobre eventos em determinados estados, por exemplo, quando um evento é concluído ou cancelado.
- Registrar em log informações sobre os atributos envolvidos em um evento. Por exemplo, você pode registrar em log os atributos que mudam durante um evento ModifyUserEvent.
- Definir o nível de auditoria do log de atributos.

Observação: para obter mais informações sobre como configurar a auditoria, consulte o *Guia de Configuração*.

Considerações sobre o CA Audit

O CA Audit é um sistema de gerenciamento de auditoria que permite coletar e armazenar dados relacionados à segurança para auditoria, geração de relatórios, verificação de conformidade e monitoramento de eventos.

Para realizar a integração com o CA Audit, instale o componente iRecorder ao instalar o Servidor do CA IdentityMinder. O iRecorder recupera eventos do CA IdentityMinder. Com base nas políticas do Gerenciador de políticas do CA Audit, o iRecorder ignora o evento ou o roteia pelo CA Audit.

Decidir requisitos de repositório de usuários

Uma implementação do CA IdentityMinder deve incluir um repositório de usuários que contenha as identidades de usuários que o CA IdentityMinder mantém. Normalmente, esse é um repositório de usuários existente que uma empresa usa para armazenar informações sobre seus usuários, como funcionários e clientes.

Se a sua implementação incluir provisionamento, o CA IdentityMinder também exigirá um diretório de provisionamento que inclua usuários globais, que são associados a contas em terminais, como Microsoft Exchange, o Active Directory e Oracle.

Como escolher uma solução de repositório de usuários

Para gerenciar um repositório de usuários existente, use o CA IdentityMinder para gerenciá-lo e, em seguida, crie um Diretório de provisionamento separado. No entanto, em implementações em que você pode escolher uma opção de repositório de usuários, considere as principais diferenças na tabela a seguir.

Importante: A CA Technologies recomenda enfaticamente o uso de um repositório de usuários separado e do Diretório de provisionamento para novas implantações.

Capacidade	Repositório de usuários separado e Diretório de provisionamento	Único repositório de usuários e Diretório de provisionamento
Suporte ao objeto de usuário	Sim	Sim (esquema personalizado)
Suporte ao objeto de grupo	Sim	Sim (esquema personalizado)
Suporte à associação ao grupo	Sim	Sim (modelo proprietário)
Suporte ao objeto de organização	Sim	Não
Suporte de provisionamento direto	Não	Sim

Capacidade	Repositório de usuários separado e Diretório de provisionamento	Único repositório de usuários e Diretório de provisionamento
Repositório de usuários adicionais exigidos para provisionamento	Sim	Não
Número de usuários recomendados:	Milhões de usuários	Dezenas de milhares de usuários

Gerenciando vários repositórios de usuários

Uma empresa pode manter vários repositórios de usuários. Em cada repositório de usuários, a identidade do usuário permite acessar diferentes recursos corporativos. Você pode usar um dos métodos a seguir para gerenciar vários repositórios de usuários:

- Use o CA IdentityMinder para gerenciar diretamente o Diretório de provisionamento e use o Servidor de provisionamento para gerenciar indiretamente os usuários e contas nos diferentes repositórios de usuários.

  Essa abordagem permite que você:

  - Gerencie de maneira centralizada os usuários que podem receber vários recursos corporativos de um local.
  - Implemente regras de negócios e de segurança em comum pelos recursos da empresa. Isso pode incluir o seguinte:
    - Controle de acesso com base em função
    - Administração delegada
    - Tarefas e telas que são personalizadas de acordo com o tipo de identidade corporativa que gerenciam
    - Políticas de identidade para gerenciamento de identidades com base em regras
    - Personalização e extensibilidade

  Observação: para obter informações sobre esses recursos, consulte o *Guia de Administração*.

- Crie um ambiente do CA IdentityMinder separado para gerenciar cada repositório de usuários

  Com esse método, as informações não são compartilhadas entre os ambientes.

Selecionar componentes a serem instalados

A tabela a seguir lista os componentes a serem instalados para oferecer suporte à funcionalidade que você deseja implementar.

Observação: para obter instruções sobre como instalar esses componentes, consulte o *Guia de Instalação*.

Se desejar...	Instale estes componentes
Gerenciar as identidades de usuário em um repositório de usuários corporativos	■ Servidor do CA IdentityMinder
Provisionar contas em sistemas do terminal	■ Servidor de provisionamento ■ Diretório de provisionamento ■ Gerenciador de provisionamento ■ Conectores ■ Servidores de conectores **Observação**: para obter instruções sobre como instalar conectores, consulte o *Guia de Conector* para o tipo de conector que você deseja instalar.
Implementar um ou mais dos recursos a seguir: ■ Autenticação avançada ■ Políticas de senha avançadas ■ Diferentes capas de console para diferentes conjuntos de usuários ■ Configurar preferências de localidade para usuários	■ Servidor de políticas do SiteMinder ■ Repositório de políticas ■ Agente web do SiteMinder ■ Extensões do CA IdentityMinder para o Servidor de políticas **Observação**: para obter instruções sobre como instalar o Servidor de políticas e o repositório de políticas do SiteMinder, consulte o *Guia de Instalação do Servidor de Políticas do CA SiteMinder Web Access Manager* .Para obter instruções sobre como instalar o Agente web, consulte o *Guia de Instalação do Agente Web do CA SiteMinder Web Access Manager* .
Gerar relatórios sobre a atividade do CA IdentityMinder	Servidor de relatórios do IAM

Decidir requisitos de hardware

O hardware necessário para uma instalação do CA IdentityMinder depende da funcionalidade que você deseja implementar e do tamanho da sua implantação.

As seções a seguir descrevem as implementações típicas do CA IdentityMinder e os respectivos hardwares necessários.

Tipos de implantação

Ao planejar o hardware necessário para uma implantação do CA IdentityMinder, considere os recursos que deseja implementar e o tamanho inicial da implantação. Use uma das categorias a seguir para estimar o tamanho da implantação.

Observação: o tipo de implantação que você seleciona determinará o tamanho do arquivo DxGrid que é usado pelo Diretório de provisionamento. Especifique o tipo de implantação ao instalar o Servidor do CA IdentityMinder.

Demonstração

Implantação de um único servidor para uso em demonstrações ou teste básico em um ambiente de desenvolvimento. Uma implantação de demonstração oferece suporte a até 10.000 contas provisionadas.

Observação: esse tipo de implementação não oferece suporte a implementações de produção.

Básica

Uma implementação de alta disponibilidade que é adequada para a maioria das implementações de pequeno e médio porte. Uma implantação básica oferece suporte a até 400.000 contas provisionadas.

Esse tipo de implementação exige dois servidores para execução do aplicativo do CA IdentityMinder e seus componentes, bem como dois servidores para execução do banco de dados e do repositório de usuários do CA IdentityMinder.

Intermediária

Uma implementação de alta disponibilidade que é adequada para implementações de tamanho médio. Uma implantação intermediária oferece suporte a até 600.000 contas provisionadas.

Grandes empresas

Uma implementação de alta disponibilidade que inclui clusters de servidores adicionais para lidar com usuários adicionais e um grande número de transações. Uma implantação grande oferece suporte a mais de 600.000 contas provisionadas.

Observação: para obter mais informações sobre implementações de alta disponibilidade, consulte o *Guia de Instalação*.

Requisitos adicionais de provisionamento

Além dos componentes exigidos para uma implementação básica do CA IdentityMinder, os seguintes componentes adicionais serão necessários quando o CA IdentityMinder incluir provisionamento:

- Servidor de provisionamento

  Pode ser instalado na mesma máquina que o servidor do CA IdentityMinder.

- Inicialização do Diretório de provisionamento

  Importante: a inicialização do Diretório de provisionamento deve ser instalada no CA Directory.

- Gerenciador de provisionamento

  Pode ser instalado em qualquer máquina Windows que possa acessar o Servidor de provisionamento.

Observação: em um ambiente de desenvolvimento, esses componentes podem ser instalados em uma máquina que também inclua os componentes da instalação básica.

Requisitos adicionais para integração do SiteMinder

Quando o CA IdentityMinder integra-se ao SiteMinder, a implementação deve incluir os componentes da instalação básica do CA IdentityMinder, além dos seguintes componentes adicionais:

- **Servidor de políticas**

  Fornece gerenciamento de políticas, bem como serviços de autenticação, autorização e contabilidade.

  O Servidor de políticas pode ser instalado no mesmo computador que o Servidor do CA IdentityMinder, se o Servidor de políticas for dedicado ao CA IdentityMinder. Se o Servidor de políticas estiver protegendo outros aplicativos, é recomendável instalá-lo em uma máquina separada para garantir melhor desempenho.

- **Repositório de políticas**

  Contém todos os dados do Servidor de políticas. Você pode configurar um repositório de políticas em um banco de dados relacional ou LDAP suportado. Em implementações de alta disponibilidade, é recomendável instalar o repositório de políticas em um servidor separado.

- **Extensões para o Servidor de políticas**

  Permite a um Servidor de políticas do SiteMinder oferecer suporte ao CA IdentityMinder. Instale as extensões em cada sistema do Servidor de políticas do SiteMinder na sua implementação do CA IdentityMinder.

- **Agente web do SiteMinder**

  Funciona com o Servidor de políticas do SiteMinder para proteger o Console de usuário. Instalado no sistema com o Servidor do CA IdentityMinder.

Escolher um método de importação de usuários

Se precisar importar usuários em um repositório de usuários existente, o método que você selecionar deverá ter como base seus requisitos de negócios.

As seções a seguir descrevem as opções para importação de usuários.

Como importar usuários em um novo repositório de usuários

Após decidir como armazenar dados do usuário, talvez você precise importar usuários de um repositório para outro. Dependendo de sua implementação, é possível usar métodos diferentes para importar usuários.

Observação: após a importação de usuários em um novo repositório de usuários, você poderá usar as políticas de identidade (na página 59) para aplicar as alterações aos usuários importados.

Importar usuários por meio do CA IdentityMinder

O CA IdentityMinder fornece os seguintes métodos para adicionar usuários a um repositório de usuários que ele gerencia diretamente.

Método	Recursos	Limitações
Carregador de itens em massa	Permite usar a tarefa do Carregador de itens em massa no Console de usuário para fazer upload de arquivos alimentadores que são usados para manipular grandes números de objetos gerenciados simultaneamente. A vantagem do método Carregador de itens em massa é a possibilidade de automatizar o processo de manipulação de um grande número de objetos gerenciados usando um arquivo de informações (alimentador). A tarefa do Carregador de itens em massa também pode ser mapeada para um processo de fluxo de trabalho.	Se você estiver usando o Carregador de itens em massa, talvez veja exceções de memória insuficiente, dependendo do número de usuários que estiver importando. Para resolver esse problema, aumente as configurações de memória da JVM.
Invocação de tarefa remota por meio do TEWS	Permite a execução de qualquer tarefa do CA IdentityMinder que esteja ativada para os Serviços web, incluindo a tarefa Criar usuário. Se a tarefa estiver configurada para Sincronização de usuários, o CA IdentityMinder executará todas as políticas de identidade aplicáveis.	As características de desempenho do modelo de serviço web podem não ser muito adequadas para os requisitos de alta taxa de transferência das operações de importação em massa.
API do IM	■ Fornece APIs com base em usuário que podem ser chamadas diretamente para a criação de usuários por meio de um cliente Java ■ Fornece a capacidade de taxa mais alta de transferência.	■ Ignora os mecanismos de auditoria e segurança fornecidos pelo Servidor de tarefas. ■ Não oferece suporte à execução de Políticas de identidade.

Observação: para obter mais informações sobre o Carregador de itens em massa, consulte o *Guia de Administração*. Para obter mais informações sobre e TEWS e a API do IM, consulte o *Guia de Programação do Java*.

Executar Políticas de identidade em usuários importados

Uma *política de identidade* é um conjunto de alterações nos negócios que ocorrem quando um usuário atende a uma determinada condição ou uma regra. Essas alterações podem incluir atribuição ou revogação de funções (incluindo funções de provisionamento para usuários no diretório de provisionamento), atribuição ou revogação da associação ao grupo e atualização de atributos em um perfil de usuário.

Você pode usar políticas de identidade para aplicar as alterações nas contas de usuário após terem sido importadas para um novo repositório de usuários.

Esta seção descreve os métodos para a execução de políticas de identidade dos usuários importados em uma ou duas etapas.

Abordagem de uma etapa

É possível usar os seguintes métodos de importação para executar políticas de identidade em usuários que você importa em um novo repositório de usuários em uma única etapa:

- Carregador de itens em massa no Console de usuário
- Execução da tarefa Criar usuário por meio do TEWS
- Sincronização de entrada

Abordagem em duas etapas

Usando uma abordagem de duas etapas, primeiramente, você importa usuários e, em seguida, executa políticas de identidade nesses usuários. É possível usar esse método quando o CA IdentityMinder gerencia usuários no Servidor de provisionamento. Esse método pode fornecer mais flexibilidade, dependendo dos seus requisitos de importação.

1. Use uma das ferramentas de importação para adicionar usuários no Diretório de provisionamento.
2. Chame a tarefa Sincronizar usuários do CA IdentityMinder por meio do TEWS em cada um dos usuários importados.

Importar usuários por meio do Servidor de provisionamento

O Servidor de provisionamento inclui opções de importação em massa para adicionar e gerenciar usuários no Diretório de provisionamento. As tabelas a seguir descrevem os métodos para importar os usuários no Diretório de provisionamento.

Método	Recursos	Limitações
Utilitário de lote (etautil)	Um utilitário da interface de linha de comando que permite gerenciar objetos no Diretório de provisionamento	■ No momento, suportado somente nos sistemas Windows
Explorar e correlacionar	■ Detecta novos objetos que o Servidor de provisionamento pode gerenciar em um terminal conhecido (incluindo usuários) ■ Fornece recursos de correlação para instâncias de objeto existentes no terminal e no Servidor de provisionamento. Informações adicionais podem ser encontradas no tópico Funcionalidade Explorar e correlacionar.	■ Por padrão, a funcionalidade Explorar e correlacionar é disponibilizada para os conectores atualmente suportados. Pode ser estendida com conectores personalizados ■ A opção Correlacionar pode afetar a escalabilidade quando se está trabalhando com uma grande variedade de populações de usuários. Se você selecionar essa opção de importação, certifique-se de avaliar as implicações de desempenho e escalabilidade.

Sincronizar usuários globais com o repositório de usuários do CA IdentityMinder

Após importar usuários no Servidor de provisionamento, você pode usar os seguintes métodos para adicionar esses usuários no repositório de usuários do CA IdentityMinder:

- **Sincronização de entrada**

  A sincronização de entrada mantém os usuários do CA IdentityMinder atualizados com as alterações que ocorrem no Diretório de provisionamento. As alterações no Diretório de provisionamento incluem as que foram realizadas usando o Gerenciador de provisionamento ou sistemas com conectores para o Servidor de provisionamento.

  Observe o seguinte ao usar a sincronização de entrada para importar usuários:

  - No Management Console do CA IdentityMinder, você pode personalizar o modo como os atributos da solicitação de entrada são mapeados para atributos na tarefa do CA IdentityMinder.

    Observação: para obter mais informações, consulte o *Guia de Administração*.

  - Considere quais alterações do Servidor de provisionamento exigem a sincronização com o repositório de usuários corporativo. A sincronização de um número grande de alterações pode afetar o desempenho e a escalabilidade.

- **Funções de provisionamento e modelos de conta**

  O Servidor de provisionamento pode gerenciar contas no repositório de usuários do CA IdentityMinder usando funções de provisionamento e modelos de conta. Isso requer que um terminal gerenciado, que aponta para o repositório de usuários do CA IdentityMinder, tenha sido adquirido e que os modelos de conta e funções apropriados existam. Nesse caso, os usuários globais criados usando uma das opções descritas em Importar usuários por meio do Servidor de provisionamento podem receber uma função de provisionamento que cria a conta de usuário no repositório de usuários do CA IdentityMinder.

Desenvolver um plano de implantação

Ao planejar uma grande implementação, é necessário implantar a funcionalidade do CA IdentityMinder em estágios. A seguinte ordem de implantação permite obter rapidamente um valor significativo do CA IdentityMinder, avaliar as necessidades em constante mudança da sua implementação ao longo do tempo e construir cuidadosamente o ambiente para obter melhor desempenho e escalabilidade:

- Gerenciamento de senhas e autoatendimento
- Políticas de identidade
- Aprovações de fluxo de trabalho

- Administração delegada para objetos de usuário, grupo ou organização
- Administração delegada para administração de funções

Após cada estágio da implantação, certifique-se de avaliar o desempenho e fazer ajustes antes de passar para a próxima etapa. A otimização do CA IdentityMinder (na página 71) fornece informações sobre desempenho, ajuste e escalabilidade.

Implantar gerenciamento de senhas e autoatendimento

Implante o gerenciamento de senhas e tarefas de autoatendimento antes de implantar outros recursos do CA IdentityMinder pelos seguintes motivos:

- O gerenciamento de senhas e tarefas de autoatendimento são fáceis de implantar e fornecem valor significativo rapidamente.
- Esses recursos são independentes do modelo da administração delegada e podem ser reconfigurados, conforme necessário para atender às necessidades de negócios em constante mudança.
- Geralmente, esses recursos geram o volume máximo de tarefas que o CA IdentityMinder processa regularmente. Por esse motivo, eles fornecem uma maneira de testar a escalabilidade da sua implementação antes de implantar recursos adicionais.

Para implantar tarefas de autoatendimento, execute as seguintes etapas:

1. Configure a tarefa de autorregistro.

   Essa é uma tarefa pública, que é ativada por padrão durante a instalação. Para configurar essa tarefa, adicione ou remova campos na tarefa de autorregistro padrão, conforme necessário.

2. Implante a função Autogerenciador.

   A regra de integrante para essa função deve estar configurada para ser aplicada a todos os usuários ou deve incluir uma regra de integrante que atribua automaticamente a função aos novos usuários. Por exemplo, você pode criar uma regra de integrante que atribua a função Autogerenciador a todos os funcionários de tempo integral. Quando um usuário se autorregistra, o CA IdentityMinder pode definir o tipo de funcionário para tempo integral (usando um manipulador de atributos lógicos ou o manipulador de tarefas de negócios). O usuário atenda aos critérios da regra de integrante e recebe automaticamente a função Autogerenciador.

   Observação: ao configurar as regras de integrante para a função Autogerenciador, não permita que os administradores adicionem ou removam integrantes da função. Como a função é atribuída automaticamente, não é necessário um administrador para definir explicitamente a função.

Para implantar recursos de gerenciamento de senhas, execute as seguintes etapas:

1. Configure as tarefas públicas de gerenciamento de senhas, como a tarefa de senha esquecida.
2. Crie políticas de senha que determinem como as senhas são criadas e quando expiram.
3. Implante a função Gerenciador de senhas, que permite que os integrantes da função redefinam as senhas dos usuários.

Observação: para obter informações sobre gerenciamento de senhas, funções e tarefas, consulte o *Guia de Administração*.

Implantar políticas de identidade

Uma política de identidade é um conjunto de alterações nos negócios que ocorrem quando um usuário atende a uma determinada condição ou uma regra. Você pode usar políticas de identidade para fornecer direitos orientados aos negócios antes que um modelo completo de delegação seja implantado. Por exemplo, você pode criar uma política de identidade que atribui a função de provisionamento Gerente de vendas, que concede acesso a aplicativos de vendas, para todos os usuários cujo cargo seja Gerente de vendas. Quando um representante de vendas é promovido a Gerente de vendas, ele recebe automaticamente o acesso a todos os sistemas necessários para realizar a tarefa sem aguardar o envolvimento do administrador.

Para implantar políticas de identidade, execute as seguintes etapas:

1. Configure políticas de identidade que são disparadas por alterações em atributos de perfil do usuário.
2. Configure a função Gerenciador de usuários para permitir que um número pequeno de administradores use as tarefas de usuário, como Criar usuário e Modificar o usuário, de modo a alterar os atributos que disparam as políticas de identidade.

   Certifique-se de configurar as regras de escopo nas políticas de integrante do Gerenciador de usuários para determinar o conjunto de usuários que os integrantes da função podem gerenciar.

Observe o seguinte ao implantar políticas de identidade:

- Considere criar, inicialmente, políticas de identidade que concedam direitos que *não* exigem aprovações de fluxo de trabalho. Isso permite que você implante políticas de identidade sem precisar definir os processos de fluxo de trabalho, formulários de aprovação, e modelos de aprovador.
- Antes de criar políticas de identidade, você deve estar familiarizado com outros métodos de implementação das regras de negócios no CA IdentityMinder, como regras de validação de dados, atributos lógicos, manipuladores de tarefas de lógica de negócios e processos de fluxo de trabalho, de modo a determinar qual método oferece a melhor solução.

  Observação: para obter mais informações sobre esses métodos, consulte o *Guia de Administração* e o *Guia de Programação do Java*.
- As políticas de identidade são uma forma eficaz de atribuir direitos no CA IdentityMinder. No entanto, elas podem afetar o desempenho de modo significativo (na página 87).
- Para a implantação inicial das tarefas do usuário, considere remover ou ocultar as guias de relacionamento, como as guias Funções, que gerenciam os mesmos direitos que as políticas de identidade. Isso evita o risco de direitos não autorizados e impede o possível impacto de desempenho de funções construídas inadequadamente.

Observação: para obter mais informações sobre políticas de identidade, consulte o *Guia de Administração*.

Implantar aprovações de fluxo de trabalho

As aprovações de fluxo de trabalho pode adicionar um nível adicional de segurança e automação para sua implementação do CA IdentityMinder.

Implantar aprovações de fluxo de trabalho exige as seguintes tarefas:

1. Decida quais eventos ou tarefas exigem aprovações.
2. Defina o conjunto de aprovadores, participantes chamados, para cada processo de fluxo de trabalho.

   Observação: todos os participantes são determinados dinamicamente pelo resolvedores participantes. Para manter um bom desempenho, limite o número de participantes a trinta usuários.
3. Configure formulários de aprovação.
4. Defina processos de fluxo de trabalho personalizados, se necessário.

Aprovações de fluxo de trabalho em nível de tarefa e ambiente

O CA IdentityMinder oferece suporte a dois tipos de aprovação: em nível de ambiente e em nível de tarefa. As aprovações em nível de ambiente são definidas para todas as instâncias de um evento, independentemente das tarefas às quais estão associadas. As aprovações em nível de tarefa são definidas para um evento específico associado a uma tarefa específica. As aprovações em nível de tarefa têm precedência sobre as aprovações em nível de ambiente.

A maioria das aprovações é definida em nível de ambiente para assegurar que as mesmas atividades de fluxo de trabalho ocorram para um evento, independentemente da tarefa à qual está associado. No entanto, nas seguintes situações, considere a implementação no do fluxo de trabalho em nível de tarefa:

- Você tem tarefas especializadas que executam alterações de negócios específicas que geram eventos e que não precisam de aprovações.
- Você tem ações de alterações, disparadas por políticas de identidade, que geram eventos que não exigem aprovação de fluxo de trabalho.
- Você precisa de flexibilidade para associar processos de fluxo de trabalho específicos a alterações específicas de tarefa.

As aprovações em nível de ambiente podem exigir recursos de sistema e processamento significativo, conforme o volume de transações aumenta. Consequentemente, isso pode trazer problemas de desempenho e escalabilidade. O uso de aprovações em nível de tarefa, quando apropriado, pode reduzir ou eliminar esses problemas.

Implantar administração delegada para usuários, grupos e organizações

A administração delegada é o gerenciamento dos usuários e dos seus respectivos direitos, com diferentes usuários do CA IdentityMinder que executam as funções de modificar, atribuir e usar uma função.

Observação: os modelos de delegação deve ser cuidadosamente criados para garantir o bom desempenho e escalabilidade em sua implementação do CA IdentityMinder.

A delegação é aplicada pelas regras de escopo, que são definidas nas políticas administrativas e de integrante para funções administrativas. Uma regra de escopo determina os objetos em que um integrante da função pode usar a função. Por exemplo, uma regra de escopo pode permitir que um Gerenciador de usuários gerencie usuários em seu departamento, mas não em outros departamentos.

Geralmente, as regras de escopo devem refletir a estrutura lógica do repositório de usuários. Por exemplo, em um repositório de usuários LDAP hierárquico, o escopo pode ser definido por organizações. Em um banco de dados relacional, o escopo pode ser definido usando atributos, como ID de departamento.

Observe o seguinte ao implantar a administração delegada para usuários, grupos e organizações:

- Limite o acesso às guias de relacionamento, como as guias Funções administrativas e Funções de provisionamento, nas tarefas relacionadas ao usuário. Essas guias de relacionamentos são incluídas nas tarefas de usuário padrão, como Criar usuário e Modificar usuário. Pense na possibilidade de removê-las das tarefas padrão e usá-las apenas em tarefas especializadas que são associados a um pequeno número de funções administrativas.
- O CA IdentityMinder avalia cada regra de escopo de forma dinâmica; informações de escopo não são armazenadas em cache. Considere a possibilidade de criar regras de escopo que contenham consultas de diretórios simples para garantir o bom desempenho.
- Avalie o desempenho das regras de escopo determinando quanto tempo o CA IdentityMinder leva para retornar os objetos que um administrador pode gerenciar.

Implantar administração delegada para funções

A administração delegada de função concede os privilégios mais significativos no CA IdentityMinder e pode ter o maior impacto (na página 72) sobre o desempenho. Por esses motivos, você deve considerar a implantação da administração delegada para funções após a implantação de todas as outras funcionalidades.

Ao implantar a administração delegada para funções, observe o seguinte:

- Limite o número de funções administrativas, os integrantes da função administrativa e os administradores da função administrativa para proteger o ambiente e garantir o bom desempenho.
- Depois de implantar a administração delegada para funções, conduza testes de escalabilidade e desempenho. Otimize o ambiente, conforme necessário.

Capítulo 5: Integração com o SiteMinder

Esta seção contém os seguintes tópicos:

SiteMinder e CA IdentityMinder

Quando o CA IdentityMinder integra-se ao CA SiteMinder, o CA SiteMinder pode adicionar as seguintes funcionalidades a um ambiente do CA IdentityMinder:

Autenticação avançada

O CA IdentityMinder inclui autenticação nativa para Ambientes do CA IdentityMinder por padrão. Os administradores do CA IdentityMinder inserem um nome de usuário e uma senha válidos para efetuar logon em um Ambiente do CA IdentityMinder. O CA IdentityMinder autentica o nome e a senha no repositório de usuários que o CA IdentityMinder gerencia.

Quando o CA IdentityMinder integra-se ao CA SiteMinder, o CA IdentityMinder usa a autenticação básica do CA SiteMinder para proteger o Ambiente. Quando você cria um Ambiente do CA IdentityMinder, um domínio da política e um esquema de autenticação são criados no CA SiteMinder para proteger o Ambiente.

Quando o CA IdentityMinder integra-se ao CA SiteMinder, também é possível usar a autenticação do SiteMinder para proteger o Management Console.

Funções e tarefas de acesso

As funções de acesso permitem que os administradores do CA IdentityMinder atribuam privilégios em aplicativos que o CA SiteMinder protege. As funções de acesso representam uma única ação que um usuário pode executar em um aplicativo de negócios, como a geração de uma ordem de compra em um aplicativo financeiro.

Mapeamento de diretório

Um administrador pode precisar gerenciar usuários cujos perfis existem em um repositório de usuários diferente daquele que é usado para autenticar o administrador. Ao efetuar logon no Ambiente do CA IdentityMinder, o administrador é autenticado usando um diretório e outro diretório para autorizar o administrador a gerenciar usuários.

Quando o CA IdentityMinder integra-se ao CA SiteMinder, é possível configurar um Ambiente do CA IdentityMinder para usar diretórios diferentes para autenticação e autorização.

Capas de diferentes conjuntos de usuários

A capa muda a aparência do Console de usuário. Quando o CA IdentityMinder integra-se ao CA SiteMinder, é possível ativar diferentes conjuntos de usuários para ver diferentes capas. Para fazer essa alteração, use uma resposta do SiteMinder para associar uma capa a um conjunto de usuários. A resposta é emparelhada com uma regra em uma política, que está associada a um conjunto de usuários. Quando a regra é acionada, ela dispara a resposta para passar informações sobre a capa ao CA IdentityMinder para criação do Console de usuário.

Observação: para obter mais informações, consulte o *Guia de Design do Console de Usuário*.

Preferências de localidade para um ambiente localizado

Quando o CA IdentityMinder integra-se ao CA SiteMinder, é possível definir a preferência de localidade para um usuário usando um cabeçalho HTTP imlanguage. No Servidor de políticas do SiteMinder, você deverá definir esse cabeçalho dentro de uma resposta do SiteMinder e especificar um atributo de usuário como o valor do cabeçalho. Esse cabeçalho imlanguage atua como a preferência de localidade de prioridade mais alta para um usuário.

Observação: para obter mais informações, consulte o *Guia de Design do Console de Usuário*.

Mais informações:

Instalação com Servidor de políticas do SiteMinder (na página 42)

Autenticação do SiteMinder

O CA IdentityMinder inclui os seguintes consoles, que devem ser protegidas:

Console de usuário

Permite que os administradores do CA IdentityMinder executem tarefas em um ambiente do CA IdentityMinder.

Console de gerenciamento

Permite que os administradores do CA IdentityMinder criem e configurem um diretório do CA IdentityMinder, um Diretório de provisionamento e um ambiente do CA IdentityMinder.

O CA IdentityMinder inclui autenticação nativa, que protege o Console de usuário por padrão. O Management Console não é protegido por padrão, mas você pode configurar o CA IdentityMinder para protegê-lo. O CA SiteMinder também pode ser usado para proteger o Management Console.

Para configurar outros tipos de autenticação para o Console de usuário, como certificado ou chave de autenticação, o CA IdentityMinder deve integrar-se ao SiteMinder.

Observação: para obter mais informações, consulte o *Guia de Configuração*.

Capítulo 6: Otimizando o CA IdentityMinder

Esta seção contém os seguintes tópicos:

Desempenho do CA IdentityMinder

O desempenho do CA IdentityMinder depende do desempenho individual de diferentes recursos e componentes.

Você pode otimizar as seguintes funcionalidades em um ambiente do CA IdentityMinder:

- Funções
- Tarefas
- Gerenciamento e associação ao grupo
- Políticas de identidade

Para ganhos adicionais de desempenho, você também pode ajustar os seguintes componentes:

- Repositório de usuários
- Componentes de provisionamento
- Componentes de tempo de execução, incluindo os bancos de dados, como o banco de dados de persistência de tarefas, e configurações do servidor de aplicativos

Para assegurar melhor desempenho, configure a funcionalidade do CA IdentityMinder usando as diretrizes nas seções a seguir. Em seguida, avalie o desempenho e ajuste os componentes, conforme necessário. Como os componentes trabalham juntos, talvez precisem ser feitas várias iterações até você encontrar o melhor ajuste para as configurações do seu ambiente.

Otimizações de função

O CA IdentityMinder inclui três tipos de função:

- Funções administrativas

  Determine os privilégios de um usuário no Console de usuário.

  Quando um usuário efetuar logon em um ambiente do CA IdentityMinder, a conta de usuário terá uma ou mais funções administrativas. Cada função administrativa contém tarefas, como Criar usuário, que um usuário pode realizar nesse ambiente do CA IdentityMinder. As funções administrativas que um usuário possui determinam a apresentação do Console de usuário, portanto, os usuários visualizam apenas as tarefas que são associadas às suas funções.

- Funções de provisionamento

  Forneça aos usuários contas em terminais gerenciados, como um sistema de email.

- Funções de acesso

  Ofereça outra maneira de fornecer direitos no CA IdentityMinder.

As funções incluem políticas que determinam o seguinte:

- Quem pode usar a função (apenas para funções administrativas e de acesso) e onde é possível usá-la
- Quem pode gerenciar os administradores e integrantes da função
- Quem pode modificar a definição de função

A avaliação de funções e de seus privilégios associados pode ter um impacto significativo sobre o desempenho do CA IdentityMinder.

Como a avaliação da função afeta o desempenho no logon

Quando um usuário do CA IdentityMinder tenta efetuar logon no Console de usuário, as seguintes ações ocorrem:

1. O CA IdentityMinder solicita ao usuário que forneça credenciais, como um nome de usuário e uma senha.
2. As credenciais de usuário são autenticadas por meio de um dos métodos a seguir:
   - Autenticação nativa do CA IdentityMinder
   - Autenticação do SiteMinder, se a implementação do CA IdentityMinder incluir o SiteMinder

3. O CA IdentityMinder avalia cada política de integrante para cada função administrativa no ambiente, de modo a determinar quais funções administrativas se aplicam ao usuário.

   Observação: essa avaliação ocorre apenas uma vez para um determinado usuário. Após a avaliação inicial, o CA IdentityMinder armazena os resultados em cache. O CA IdentityMinder usa as informações armazenadas em cache até que ocorra uma alteração no usuário ou no conjunto de políticas de integrante, o que faz com que o CA IdentityMinder atualize as informações no cache.

4. O Console de usuário do CA IdentityMinder exibe as categorias que o usuário pode exibir com base em suas funções.

Esse processo ocorre para cada usuário que efetua logon no Console de usuário. Se um ambiente do CA IdentityMinder contiver uma grande quantidade de funções, ou políticas de integrante ineficientes, a avaliação de associação à função poderá afetar significativamente o desempenho. Nesse caso, a tela inicial exibida para os usuários quando eles efetuam logon no Console de usuário pode ser mostrada lentamente.

Observação: o CA IdentityMinder não precisa avaliar políticas de integrante quando um usuário acessa uma tarefa pública para se autorregistrar ou solicitar uma senha esquecida. Nesses casos, o CA IdentityMinder não precisa de uma lista de funções do usuário, pois ele não exibe o Console de usuário completamente.

Desempenho e objetos de função

Para oferecer suporte a cada função, o CA IdentityMinder cria vários objetos no repositório de objetos (na página 34) do CA IdentityMinder, dependendo da configuração da função.

O CA IdentityMinder cria um objeto base para cada função. Além do objeto base, o CA IdentityMinder cria um objeto para cada política.

Grandes quantidades de objetos de função podem afetar o desempenho das avaliações de política e buscas no repositório de objetos.

Desempenho do repositório de objetos

O CA IdentityMinder armazena informações necessárias para gerenciar usuários e direitos em um repositório de objetos. Ter uma grande quantidade de objetos de função no repositório de objetos pode causar os seguintes problemas:

- Pesquisas por objetos gerenciados nas telas de tarefas do CA IdentityMinder podem demorar mais.

  Para reduzir o impacto em pesquisas, indexe atributos usados nas pesquisas (na página 91).

- As tarefas de gerenciamento de funções podem ser executadas lentamente.

  Alguns exemplos de tarefas de gerenciamento de funções que são afetadas por um repositório de objetos amplo incluem:

  - A tarefa Criar função administrativa fica lenta porque o CA IdentityMinder deve verificar se o nome da função é exclusivo no repositório de objetos.
  - A tarefa Excluir função administrativa deve remover todos os objetos criados para oferecer suporte à função e o cache de objetos deve ser atualizado.

- O CA IdentityMinder leva muito tempo para avaliar políticas de função.

O CA IdentityMinder armazena informações em cache no repositório de objetos para melhorar o desempenho.

Otimizar avaliação da política de função

Para cada função administrativa, você pode criar três tipos de políticas:

- Políticas de integrante

  Defina uma regra de integrante, que determina os usuários que recebem a função, e as regras de escopo, que determinam os objetos que os integrantes da função podem gerenciar

- Políticas administrativas

  Defina regras administrativas, regras de escopo e privilégios de administrador para uma função

- Políticas de proprietário

  Defina quem pode modificar uma função

Para otimizar o desempenho quando o CA IdentityMinder avalia políticas de função, considere o seguinte:

- Limite o número de funções administrativas em um ambiente do CA IdentityMinder.
- Siga as diretrizes para a criação de regras de políticas (na página 75).
- Ajuste o repositório de usuários.
- Ajuste o repositório de políticas, se o CA IdentityMinder incluir o SiteMinder.

Diretrizes para criação de regra de política

Um dos principais fatores para determinar o desempenho geral das avaliações de política de função é o tempo necessário para avaliar uma regra de política. Para melhorar o tempo de avaliação de regras de política, observe o seguinte ao criar uma política:

- Quando possível, limite o número de objetos de política que o CA IdentityMinder cria e o número de buscas no repositório de usuários que ele executa ao criar regras de políticas com expressões complexas.

  Uma única regra com uma expressão complexa é mais eficiente do que várias regras com expressões simples.
- Quando possível, selecione o tipo de regra de política mais eficiente e expansível.
- Ative a opção de avaliação na memória para regras de política.

  A opção de avaliação na memória reduz significativamente o tempo de avaliação da política ao recuperar informações sobre um usuário a ser avaliado no repositório de usuários e ao armazenar uma representação desse usuário na memória. O CA IdentityMinder usa a representação na memória para comparar valores de atributo em relação às regras da política.

  Observação: para obter mais informações sobre a opção de avaliação na memória, consulte o *Guia de Configuração*.
- Ajuste o repositório de usuários.
- Ajuste o repositório de políticas, se a sua implementação do CA IdentityMinder incluir o SiteMinder.

Limitar objetos de política e pesquisas no repositório de usuários

Cada regra em uma política de função exige um conjunto de objetos no repositório de objetos. Quando o CA IdentityMinder avalia uma regra, ele carrega esses objetos e realiza buscas necessárias no repositório de usuários.

O exemplo a seguir mostra uma política de integrante que inclui três regras de integrante. Cada regra inclui quatro regras de escopo.

Member Policies

Member Rule	Scope Rules
where (Department = "Engineering")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")
where (Department = "Human Resources")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")
where (Department = "Administration")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")

Nesse exemplo, CA IdentityMinder cria os objetos e executa as buscas no repositório de usuários descritas na tabela a seguir ao avaliar e aplicar a política de integrante.

Regra	Objetos de política	Possíveis pesquisas no repositório de usuários
■ Regra de integrante: onde (Departamento = "Administração") ■ Escopo do usuário: Cidade = "Boston" ■ Escopo do grupo: Nome do grupo = "Equipe do produto" ■ Escopo da função de provisionamento: Nome = "Funcionário" ■ Escopo da tarefa de acesso: Nome = "Desenvolvimento"	5	5 (uma para cada objeto de definição de regra)
■ Regra de integrante: onde (Departamento = "Engenharia") ■ Escopo do usuário: Cidade = "Boston" ■ Escopo do grupo: Nome do grupo = "Equipe do produto" ■ Escopo da função de provisionamento: Nome = "Funcionário" ■ Escopo da tarefa de acesso: Nome = "Desenvolvimento"	5	5
■ Regra de integrante: onde (Departamento = "Recursos Humanos") ■ Escopo do usuário: Cidade = "Boston" ■ Escopo do grupo: Nome do grupo = "Equipe do produto" ■ Escopo da função de provisionamento: Nome = "Funcionário" ■ Escopo da tarefa de acesso: Nome = "Desenvolvimento"	5	5

Nesse exemplo, o CA IdentityMinder cria 15 objetos e executa 15 pesquisas de diretório para determinar a associação e o escopo.

Para limitar o número de objetos de política e de pesquisas no repositório de usuários que o CA IdentityMinder executa, combine regras em expressões complexas. O exemplo abaixo especifica os mesmos direitos do primeiro exemplo como uma regra de integrante.

Member Policies

Member Rule	Scope Rules
where (Department = "Administration" or Department = "Engineering" or Department = "Human Resources")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")

Nesse exemplo, o CA IdentityMinder cria apenas dez objetos de política e executa apenas cinco pesquisas no repositório de usuários.

Regra	Objetos de política	Possíveis pesquisas no repositório de usuários
■ Regra de integrante: onde (Departamento) = "Administração") OU onde (Departamento) = "Engenharia") OU onde (Departamento = "Recursos Humanos") ■ Escopo do usuário: Cidade = "Boston" ■ Escopo do grupo: Nome do grupo = "Equipe do produto" ■ Escopo da função de provisionamento: Nome = "Funcionário" ■ Escopo da tarefa de acesso: Nome = "Desenvolvimento"	5	5

Selecionar tipos de regra de política expansíveis

Além do número de regras de política, o tipo de regra de política também pode afetar o desempenho. Geralmente, as regras de política são criadas com base em como o repositório de usuários está estruturado e como os direitos são determinados. Por exemplo, você pode criar regras de política com base na associação ao grupo, na organização ou nos atributos de usuário. No entanto, quando existem várias maneiras de criar regras de política, considere as diretrizes de desempenho na tabela a seguir, antes de decidir o tipo de regra a ser construído.

Observação: os tipos de regra de política na tabela a seguir são listadas na ordem de desempenho, começando com o tipo de regra mais eficiente.

Tipo de regra de política	Observações de desempenho
Organização	■ Melhor desempenho geral ■ Não exige uma pesquisa em diretórios LDAP. O CA IdentityMinder usa o DN do usuário que está sendo avaliado e o DN da organização na regra de política
Função	■ O CA IdentityMinder armazena informações de objeto de função e as avaliações anteriores no cache do repositório de objetos ■ Na maioria dos casos, o desempenho será tão bom quanto as regras de política de organização
Atributo do usuário	■ Fornece o melhor desempenho de pesquisa no repositório de usuários, sendo a menos afetada por grandes populações de usuários ■ Permite ativar a avaliação na memória para ganhos significativos de desempenho
Associação ao grupo	■ O desempenho depende do tamanho do grupo e do tipo de repositório de usuários

Otimizações de tarefa

No CA IdentityMinder, as tarefas que um usuário visualiza no Console de usuário dependem dos privilégios específicos desse usuário. Para exibir e executar tarefas, o CA IdentityMinder deve realizar várias avaliações de segurança, o que pode ter um impacto significativo no desempenho quando aplicadas a todos os usuários em um ambiente do CA IdentityMinder.

O CA IdentityMinder executa avaliações de segurança quando ocorrem as seguintes ações:

- O usuário efetua logon no Console de usuário

  Nesse caso, o CA IdentityMinder deve avaliar as funções do usuário para determinar quais tarefas esse usuário pode acessar no Console de usuário.

- Um usuário chama uma tarefa

  Quando uma tarefa é chamada, o CA IdentityMinder deve determinar quais objetos esse usuário pode gerenciar com essa tarefa.

- Um usuário acessa uma guia de relacionamento

  Um guia de relacionamento é qualquer guia em que um usuário pode exibir ou gerenciar um relacionamento um-para-muitos entre a entidade da tarefa e um conjunto de direitos. Um exemplo de uma guia de relacionamento é a guia Funções administrativas, que exibe as funções que um usuário tem.

- Um usuário adiciona objetos em uma guia de relacionamento

  Por exemplo, o CA IdentityMinder executa verificações de segurança adicionais quando um usuário adiciona mais funções para outro usuário na guia Funções administrativas.

O desempenho da tarefa é afetado pelo seguinte:

- Escopo da tarefa, que determina onde um administrador pode usar uma tarefa
- Guias de relacionamento, que exibem um relacionamento do objeto com outros objetos

Avaliação e desempenho do escopo da tarefa

Quando um administrador usa uma tarefa administrativa que envolva procurar um objeto gerenciado, como um usuário, grupo, organização, tarefa ou função, o CA IdentityMinder avalia e aplica as regras do escopo da tarefa. Essas regras podem afetar significativamente o tempo que o CA IdentityMinder leva para exibir a lista de objetos a serem selecionados para a tarefa.

Observação: diferentemente das avaliações de política de integrante, administrativa e de proprietário, as informações sobre avaliações de regra de escopo não são armazenadas em um cache.

O escopo da tarefa é determinado pelo seguinte:

- Tipo de objeto que a tarefa gerencia.
- Regras de escopo que se aplicam à função administrativa que inclui a tarefa. As regras de escopo são definidas nas políticas administrativas, de integrante e de proprietário.
- Critérios de pesquisa definidos pelo usuário.

Por exemplo, considere uma tarefa Modificar usuário, que é incluída na função Gerenciador de usuários. A função Gerenciador de usuários tem uma política de integrante com uma regra de escopo que permite aos Gerenciadores de usuários gerenciar usuários na organização Funcionários. Um administrador abre a tarefa Modificar usuário e insere os critérios de pesquisa: sobrenome que comece com A. Nesse caso, o escopo para a tarefa Modificar o usuário inclui todos os usuários na organização Funcionários cujos sobrenomes comecem com A.

Como o CA IdentityMinder processa as guias de relacionamento

Uma guia de relacionamento permite que os usuários exibam e gerenciem o relacionamento que a entidade de uma tarefa tem com um conjunto de direitos. Por exemplo, a guia Funções de provisionamento mostra as funções de provisionamento que um usuário tem.

Para determinar os objetos que são exibidos em uma guia de relacionamento, o CA IdentityMinder executa várias avaliações de segurança, que podem afetar significativamente o desempenho.

O exemplo a seguir mostra as etapas que o CA IdentityMinder executa para processar a guia Funções de provisionamento:

1. Um administrador clica na guia Funções de provisionamento na tarefa Modificar usuário.
2. O CA IdentityMinder recupera as funções de provisionamento onde o usuário selecionado é um integrante.
3. Se a guia estiver configurada para permitir o gerenciamento de administradores de função, o CA IdentityMinder fará uma segunda chamada para recuperar a lista de funções de provisionamento em que o usuário selecionado é um administrador.
4. O CA IdentityMinder avalia cada função de provisionamento que o usuário possui para verificar se o administrador que iniciou a tarefa pode gerenciar a associação dessa função.

   Se o administrador puder gerenciar os integrantes da função, o CA IdentityMinder exibirá uma caixa de seleção ativa na coluna Associação para essa função na lista de funções da guia.
5. O CA IdentityMinder avalia cada função de provisionamento que o usuário possui para verificar se o administrador que iniciou a tarefa pode gerenciar os direitos administrativos dessa função.

   Se o administrador puder gerenciar os direitos administrativos, o CA IdentityMinder exibirá uma caixa de seleção ativa na coluna Administrador para essa função na lista de funções da guia.

   O CA IdentityMinder deve concluir as etapas de 2 a 5 para exibir as funções de provisionamento que o usuário possui no momento. Se o administrador precisa atribuir uma nova função de provisionamento, as etapas adicionais a seguir serão obrigatórios.
6. Ele clica no botão Adicionar para localizar novas funções de provisionamento a serem atribuídas.
7. O CA IdentityMinder exibe uma tela de pesquisa que o administrador pode usar para procurar a função a ser adicionada.
8. O administrador insere um filtro de pesquisa para localizar a função a ser adicionada.

9. O CA IdentityMinder retorna a lista de funções de provisionamento que atendem aos seguintes critérios:
   - As funções correspondem ao filtro de pesquisa inserido pelo administrador.
   - O administrador pode gerenciar a associação das funções.
   - O usuário está no escopo administrativo do administrador para as funções.
   - O usuário ainda não tem as funções de provisionamento.
10. O CA IdentityMinder repete a etapa 9 para determinar as funções onde o administrador pode gerenciar privilégios administrativos.

Guias de relacionamento e desempenho

Devido ao número de avaliações de segurança que o CA IdentityMinder executa, o processamento de uma guia de relacionamento pode afetar significativamente o desempenho. Os fatores que determinam o desempenho variam de acordo com o tipo da guia.

Para guias de relacionamentos de função, os seguintes fatores podem afetar o desempenho:

- Número de funções nas quais a entidade da tarefa é um integrante
- Número de funções nas quais a entidade da tarefa é um administrador
- Número total de objetos no sistema que o CA IdentityMinder exige para calcular as funções da entidade
- Número de políticas administrativas/de integrante por função
- Complexidade das regras de escopo da política administrativa/de integrante
- A capacidade de manter as autorizações em cache para os invocadores de tarefa limita o efeito das aplicações de segurança

Para determinar a associação ao grupo e os privilégios administrativos nas guias de relacionamento de grupo, o CA IdentityMinder deve pesquisar todos os grupos no repositório de usuários. O desempenho dessas pesquisas depende dos seguintes fatores:

- Número de objetos de grupo no repositório de usuários
- Número de integrantes de qualquer grupo
- Desempenho do banco de dados ou diretório onde está o repositório de usuários

Processamento de tarefas e desempenho

As tarefas administrativas incluem eventos, ações que o CA IdentityMinder executa para concluir a tarefa. Uma tarefa pode incluir vários eventos. Por exemplo, a tarefa Criar usuário pode incluir eventos que criam o perfil do usuário, adicionam o usuário a um grupo e atribuem funções.

Quando o CA IdentityMinder processa uma tarefa, ele processa cada evento associado à tarefa. Durante o processamento do evento, o CA IdentityMinder salva cada evento quatro vezes. Isso permite que o CA IdentityMinder preserve ações em andamento no caso de um desligamento inesperado do sistema.

Quando o CA IdentityMinder processa os diversos eventos ao mesmo tempo, os eventos são adicionados a uma fila. Quando o primeiro evento conclui o primeiro estágio de seu ciclo de vida, ele é salvo e depois movido para o fim fila para aguardar o início do segundo estágio do processamento. O CA IdentityMinder então conclui o primeiro estágio do processamento para o próximo evento na fila e esse evento é movido para o fim da fila. O processo continua até que todos os eventos na fila tenham concluído o primeiro estágio do processamento. Em seguida, o primeiro evento na fila começa a segunda fase do processamento. Isso continua até que todos os eventos na fila concluam todos os quatro estágios do processamento.

Em condições de carregamento normal, esse comportamento não afeta o desempenho. No entanto, se o sistema estiver processando um grande número de tarefas e eventos, por exemplo, durante o carregamento em massa de uma grande população de usuários, cada evento e tarefa deve esperar mais na fila e, portanto, o tempo de conclusão é mais longo.

Para evitar problemas de desempenho sob condições de carregamento, considere as seguintes ações:

- Use a configuração de Prioridade da tarefa na guia Perfil de uma tarefa.

  A configuração Prioridade da tarefa permite definir a prioridade de uma tarefa para Alta, Média ou Baixa.

  As tarefas que precisam ser processadas imediatamente devem ser definidas como Alta. As tarefas envolvidas no carregamento em massa devem ser definidas como Baixa.

  Se uma prioridade da tarefa for definido, os eventos associados à ela serão processados com outras tarefas que têm a mesma prioridade. Por exemplo, se a tarefa Modificar usuário for definida para prioridade Alta e um administrador modificar um perfil de usuário, o CA IdentityMinder processará essa tarefa antes das tarefas com prioridade Média ou Baixa. Se houver outras tarefas de prioridade Alta, o CA IdentityMinder concluirá o primeiro estágio do processamento para o primeiro evento de prioridade Alta e, em seguida, moverá esse evento para o fim da lista de outros eventos de prioridade Alta.

- Instale um Servidor do CA IdentityMinder separado e dedicado para manipular as operações de carregamento em massa.

Diretrizes para otimização de tarefas

As tarefas padrão, que o CA IdentityMinder implanta ao criar um ambiente do CA IdentityMinder, são configuradas para oferecer suporte a uma grande variedade de casos de uso de administração. A maioria das implementações do CA IdentityMinder não exigem toda a funcionalidade fornecida nas tarefas padrão. Após a criação de um ambiente do CA IdentityMinder, modifique essas tarefas para atender às necessidades específicas de administração.

As etapas a seguir fornecem diretrizes para modificar tarefas:

- **Criar tarefas de gerenciamento de usuários especializadas**

  As tarefas padrão Criar usuário, Modificar usuário e Exibir usuários fornecem recursos administrativos completos. Na maioria das implementações, apenas um pequeno número de administradores precisa de todos os recursos disponíveis.

  Crie novas tarefas que incluem apenas os recursos necessários. Por exemplo, se a maioria das tarefas de gerenciamento de usuários envolver apenas o gerenciamento de grupos e perfis, crie uma nova tarefa Modificar usuário que inclua apenas as guias Perfil e Grupo. Remova as guias Funções administrativas, Funções do acesso e Funções de provisionamento, que estão disponíveis na tarefa padrão Modificar usuário.

  As guias não usadas podem causar sobrecarga considerável se forem deixadas nas tarefas usadas frequentemente. Isso vale especialmente quando se usa um cliente do TEWS, onde essas guias podem ser ativadas inadvertidamente por meio da classe Java tab, que é fornecida com o CA IdentityMinder.

  As tarefas especializadas que você cria devem corresponder ao modelo de administração delegada (na página 66) definido para o seu ambiente.

- **Desativar Gerenciar administradores nas guias de relacionamento**

  Por padrão, todas as guias de relacionamentos fornecem a capacidade de gerenciar direitos administrativos para o objeto que a guia gerencia, como funções e grupos. A maioria das implementações não precisa fornecer essa funcionalidade aos administradores.

  Para eliminar a sobrecarga adicional que ocorre quando o CA IdentityMinder avalia direitos administrativos, desmarque a opção Gerenciar administradores nas guias a seguir, se essa funcionalidade não for necessária:

  - Funções administrativas
  - Funções de provisionamento
  - Funções de acesso
  - Grupos

  Para permitir que os usuários gerenciem direitos administrativos em guias específicas, crie cópias das guias padrão, ative a opção Gerenciar administradores e desative a opção Gerenciar integrantes. Adicione as novas guias às tarefas especializadas, que são usadas somente por administradores que precisam delas.

- **Ativar pesquisas com escopo nas guia de relacionamento de função**

  É possível configurar cada guia de função para incluir as pesquisas que permitem aos administradores especificar critérios para novas funções a serem atribuídas a um usuário. As pesquisas de função limitam o número de regras de política de integrantes e administrativa que o CA IdentityMinder deve avaliar para determinar quais funções um administrador pode atribuir a um usuário.

- **Definir opções de sincronização de tarefas**

  Para cada tarefa do CA IdentityMinder, é possível especificar uma opção de sincronização de usuários, que sincroniza os usuários com políticas de identidade, e uma opção de sincronização de contas de provisionamento, que sincroniza os usuários com contas provisionadas. As opções permitem sincronizar usuários quando uma tarefa ou um evento é concluído.

  Para eliminar o tempo de avaliação e processamento, defina a sincronização para ocorrer quando uma tarefa for concluída, em vez de quando os eventos forem concluídos.

Diretrizes para otimizações de administrador/integrante do grupo

Para melhorar o desempenho de pesquisas por integrantes e administradores do grupo, considere o seguinte:

- Defina atributos conhecidos no arquivo de configuração de diretório (directory.xml), que descreve a estrutura e o conteúdo do repositório de usuários para o CA IdentityMinder.

  Um atributo conhecido é um atributo que tem um significado especial no CA IdentityMinder.

  Para melhorar as pesquisas por administrador/integrante do grupo, defina os seguintes atributos conhecidos para o objeto de usuário:

  %MEMBER_OF%

  Identifica um atributo no objeto do usuário que armazena uma lista de grupos quando o usuário é um integrante.

  Quando definido, esse atributo podem impedir que o CA IdentityMinder pesquise todos os integrantes de todos os grupos no repositório de usuários. As pesquisas no grupo podem afetar significativamente o desempenho em grupos muito grandes.

  %ADMINISTRATOR_OF%

  Identifica um atributo no objeto do usuário que armazena uma lista de grupos quando o usuário é um administrador.

  Assim como o atributo %MEMBER_OF%, esse atributo conhecido pode eliminar as pesquisas em grupos amplos.

- Especifique o tipo de grupo no arquivo de configuração de diretório

  O CA IdentityMinder oferece suporte a três tipos de grupo: grupos padrão, grupos aninhados de grupos dinâmicos.

  Ao definir o objeto de grupo no arquivo de configuração de diretório, você pode especificar o tipo de grupo ao qual o repositório de usuários oferecerá suporte. Se a sua implementação não oferecer suporte a grupos dinâmicos ou aninhados, defina o atributo Tipo de grupo da seguinte maneira:

  GroupType = NONE

  A configuração NONE especifica o suporte para grupos padrão.

  A configuração padrão de Tipo de grupo é ALL, o que pode comprometer o desempenho.

  Observação: para obter mais informações sobre tipos de grupo e atributos conhecidos no arquivo de configuração de diretório, consulte o *Guia de Configuração*.

- Defina os índices de cache do Diretório de provisionamento para melhorar o desempenho de GlobalGroup

  Para implementações do CA IdentityMinder que incluam uma combinação de repositório de usuários e do Diretório de provisionamento, a associação a GlobalGroup pode ser otimizada para avaliação de regras de políticas de políticas de funções e identidade.

  Para ativar essa otimização, indexe os seguintes atributos, que o Servidor de provisionamento usa para resolver a associação ao grupo, no cache do Diretório de provisionamento:

  eTID

  O atributo exclusivo de ID de objeto. Para pesquisas de associação ao grupo, o valor é um usuário ou grupo específico envolvido na pesquisa.

  eTPID

  A ID pai do objeto usado ao procurar pelos relacionamentos de associação.

  eTCID

  A ID filho do objeto usado ao procurar pelos relacionamentos de associação.

Além disso, adicione as seguintes entradas de hash:

eTSuperiorClass

O tipo do objeto pai em uma pesquisa de associação

eTSubordinateClass

O tipo do objeto filho em uma pesquisa de associação

Observação: para obter mais informações sobre o cache do Diretório de provisionamento, consulte o *Guia de Instalação*.

Otimizações de política de identidade

Uma *política de identidade* é um conjunto de alterações nos negócios que ocorrem quando um usuário atende a uma determinada condição ou uma regra. Essas alterações podem incluir atribuição ou revogação de funções, atribuição ou revogação de associação ao grupo e atualização de atributos em um perfil de usuário.

O CA IdentityMinder avalia políticas de identidade quando ocorre a sincronização de usuários.

O desempenho da política de identidade é afetado pelo seguinte:

- Como as políticas de identidade são configuradas
- Com que frequência ocorre a sincronização de usuários

Como usuários e políticas de identidade são sincronizados

Ao usar políticas de identidade, é importante compreender como o CA IdentityMinder avalia e aplica as políticas aos usuários. Sem um entendimento completo do processo de sincronização de usuário, você poderá configurar conjuntos de políticas de identidade que geram resultados inesperados.

O procedimento a seguir descreve como o CA IdentityMinder avalia e aplica políticas de identidade:

1. O processo de sincronização de usuário é iniciado:
   - **Automaticamente** — É possível configurar as tarefas do CA IdentityMinder para acionar automaticamente a sincronização de usuário
   - **Manualmente** — Use a tarefa Sincronizar usuário no console de usuário para sincronizar um usuário.
2. O CA IdentityMinder determina o conjunto de políticas de identidade que se aplicam a um usuário.

3. O CA IdentityMinder compara o conjunto de políticas de identidade que se aplica a um usuário com a lista de políticas que já foram aplicadas a esse usuário.

   Observação: a lista de políticas que já foram aplicadas a um usuário é armazenada no conhecido atributo %IDENTITY_POLICY% no perfil de usuário. Para obter informações sobre como configurar esse atributo, consulte o *Guia de Configuração*.

   - Se uma política de identidade estiver na lista de políticas aplicáveis, *e* a política *não* tiver sido aplicada ao usuário anteriormente, o CA IdentityMinder adicionará a política a uma lista de alocação.
   - Se uma política de identidade estiver na lista de políticas aplicáveis, a política tiver sido aplicada ao usuário anteriormente e a configuração Aplicar uma vez para a política estiver desativada, o CA IdentityMinder adicionará a política a uma lista de realocação.
   - Se uma política de identidade não estiver na lista de políticas aplicáveis, a política tiver sido aplicada ao usuário e o usuário deixar de corresponder à condição da política. O CA IdentityMinder adicionará essas políticas a uma lista de desalocação.

4. Depois que o CA IdentityMinder avaliar todas as políticas para um usuário, aplicará as políticas na seguinte ordem:

   a. Políticas de identidade da lista de desalocação

   b. Políticas de identidade da lista de alocação

   c. Políticas de identidade da lista de realocação

5. Depois que as políticas de identidade tiverem sido aplicadas, o CA IdentityMinder reavaliará as políticas para ver se outras alterações serão necessárias com base nas alterações que ocorreram no primeiro processo de sincronização (etapas de 2 a 4).

   Isso é feito para garantir que as alterações realizadas através da aplicação de políticas de identidade não acionem outras políticas de identidade.

6. O CA IdentityMinder continua a reavaliar e aplicar políticas de identidade até que o usuário seja sincronizado com todas as políticas aplicáveis, ou até que o CA IdentityMinder atinja o nível máximo de recursão, que é definido no Management Console.

   Por exemplo, uma política de identidade pode alterar o departamento de um usuário quando o usuário recebe uma função. O novo departamento dispara outra política de identidade. No entanto, se o nível de recursão for definido como 1, a alteração subsequente não será feita até que o usuário seja sincronizado novamente.

   Para obter mais informações sobre como definir o nível de recursão, consulte a Ajuda online do Management Console.

Criar políticas de identidade eficientes

Use as seguintes diretrizes ao criar políticas de identidade:

- **Limitar o número de objetos de política**

  O CA IdentityMinder cria objetos no repositório de objetos que oferecem suporte a políticas de identidade. Para reduzir o número de objetos no repositório de objetos, crie políticas de identidade com expressões complexas.
  Uma abordagem semelhante é recomendado para políticas de função (na página 76).

- **Limitar iterações do conjunto de políticas de identidade**

  Você pode configurar o nível de recursão para uma política de identidade, o que determina o número de vezes que o CA IdentityMinder avalia e aplica políticas de identidade quando um usuário é sincronizado. Por exemplo, uma política de identidade pode alterar o departamento de um usuário quando o usuário recebe uma função. O novo departamento dispara outra política de identidade. No entanto, se o nível de recursão for definido como 1, a alteração subsequente não será feita até que o usuário seja sincronizado novamente.

  Definir o nível de recursão limita o número de vezes que o CA IdentityMinder deve avaliar políticas de identidade.

- **Limitar dependências entre regras de política de identidade**

  Você pode criar uma política de identidade onde a ação de alteração (Ação ao aplicar a política ou Ação ao remover a política) de uma política é usada na condição de política de identidade de outra política, conforme mostrado na tabela a seguir.

Condição da política de identidade	Ação ao aplicar a política	Ação ao remover a política
onde (Código de tarefa = "100")	Transformar em integrante da (função de provisionamento "Gerente da conta")	Remover integrante da (função de provisionamento "Gerente da conta")
Quem são os integrantes da (função de provisionamento "Gerente da conta")	Transformar em integrante do (grupo de "Gerentes da conta")	Remover integrante do (grupo de "Gerentes da conta")

Quando o CA IdentityMinder avalia esse tipo de política, ele deve avaliar e aplicar as alterações ao menos duas vezes para garantir que ambas as condições sejam atendidas. O nível de recursão, que é definido por todo o ambiente do CA IdentityMinder, deve ser maior que 1, o que gera avaliações adicionais para cada conjunto de políticas de identidade.

Limitar as tarefas que disparam a sincronização de usuários

As políticas de identidade são avaliadas e aplicadas durante o processo de sincronização de usuários. Você pode configurar a sincronização automática especificando uma das seguintes opções de sincronização de usuários para uma tarefa:

Ao concluir a tarefa

O CA IdentityMinder inicia o processo de sincronização de usuários quando todos os eventos em uma tarefa forem concluídos.

Em cada evento

O CA IdentityMinder inicia o processo de sincronização de usuários quando cada evento em uma tarefa é concluído.

Para obter melhor desempenho, limite o número de tarefas que disparam a sincronização automática de usuários.

Leve em consideração os seguintes pontos ao configurar a sincronização de usuários:

- **Desativar sincronização de usuários para tarefas de senha**

  Na maioria dos casos, as senhas não serão usadas em condições de política de identidade.

- **Desativar sincronização de usuários para a tarefa Sincronizar usuário**

  Como a tarefa Sincronizar usuário dispara as avaliações de política de identidade, o CA IdentityMinder executará as avaliações novamente se a opção de sincronização de usuários for ativada para essa tarefa.

- **Criar tarefas especializadas**

  Quando possível, crie tarefas que executem modificações que disparam condições de política de identidade e ative as sincronizações de usuários apenas para essas tarefas.

Otimizar avaliação de regra da política de identidade

Para reduzir o tempo de avaliação para as condições de política identidade que incluem atributos de usuário, é possível ativar uma opção de avaliação na memória. Quando a opção de avaliação na memória estiver ativada, o CA IdentityMinder irá recuperar informações sobre um usuário a ser avaliado do repositório de usuários e armazenará uma representação desse usuário na memória. O CA IdentityMinder usa a representação na memória para comparar valores de atributo em relação às condições da política. Isso limita o número de chamadas que o CA IdentityMinder faz diretamente para o repositório de usuários.

Observação: para obter mais informações sobre a opção de avaliação na memória, consulte o *Guia de Configuração*.

Ajuste do repositório de usuários

O ajuste do repositório de usuários envolve diversas etapas, incluindo:

- Otimização da estrutura do repositório de usuários
- Ajuste dos repositórios subjacentes
- Implementação de balanceamento de carga e replicação

Essas etapas dependem do tipo de repositório de usuários que você está usando. Para obter informações de ajuste dessas áreas, consulte a documentação do banco de dados ou diretório que contém o repositório de usuários.

Além das considerações gerais de ajuste, as considerações de ajuste a seguir são específicas ao CA IdentityMinder:

- **Avaliar desempenho da pesquisa do repositório de usuários**

  Para obter melhor desempenho, as pesquisas de avaliação de política do CA IdentityMinder devem ser concluídas entre 10 e 20 milissegundos.

  Para assegurar que o CA IdentityMinder possa concluir essas pesquisas de forma consistente no tempo recomendado, considere o teste de desempenho da pesquisa em várias condições de carregamento.

  Você também pode usar essa medição para determinar quando um repositório de usuários atinge seus limites físicos e servidores adicionais são necessários para balanceamento de carga.

- **Indexar atributos**

  Indexe cada atributo que é usado em uma política de função ou política de identidade. A indexação de atributos pode proporcionar melhorias significativas de desempenho.

  Observação: para obter informações sobre a indexação de atributos, consulte a documentação do diretório LDAP ou banco de dados relacional que contém o repositório de usuários.

- **Armazenar em cache os vínculos LDAP**

  No CA IdentityMinder, todos os vínculos LDAP do diretório são executados pelo usuário proxy definido no objeto de Diretório do CA IdentityMinder. Para cada conexão, o mesmo vínculo LDAP ocorre para esse mesmo usuário repetidamente.

  Se você estiver usando um diretório LDAP como um repositório de usuários, configure o diretório para armazenar em cache os vínculos LDAP (ou sessões), se o diretório oferecer suporte ao cache.

- **Ativar caches de repositório de usuários**

  Quando o CA IdentityMinder avalia as decisões de política para um usuário, as informações são armazenadas em um cache de autorização. Quando as informações em cache expiram, o CA IdentityMinder avalia todas as políticas para esse usuário novamente.

  Para melhorar o desempenho das pesquisas no repositório de usuários em avaliações de regra de política subsequentes, ative o repositório de usuários para armazenar em cache os dados pesquisados, se o repositório de usuários oferecer suporte ao cache.

  O CA Directory inclui um cache, chamado dxCache, que é uma implementação de banco de dados na memória que pode pesquisar os dados em cache.

  Observação: para obter mais informações sobre o CA Directory, consulte o *Guia do Administrador do CA Directory*.

Ajuste de componentes do provisionamento

Quando uma implementação do CA IdentityMinder inclui provisionamento, use as otimizações a seguir para garantir o melhor desempenho:

- Otimizar a conexão entre o Servidor do CA IdentityMinder e o Servidor de provisionamento

  O CA IdentityMinder se comunica com o servidor de provisionamento por meio da API do Java IAM (JIAM). Para melhorar o desempenho de comunicação, você pode configurar o seguinte:

  - Pool de sessões JIAM para várias conexões com o Servidor de provisionamento

    Observação: a CA recomenda definir o valor das sessões iniciais para 8 e o número máximo de sessões para 128.

  - Cache do JIAM para objetos recuperados do Servidor de provisionamento

  Observação: para obter informações sobre as definições de configuração do JIAM, consulte o *Guia de Administração*.

- Definir sincronização de conta para ocorrer no final de uma tarefa (na página 84), e não no final de cada evento
- Ajustar o Servidor de provisionamento

  Observação: consulte o *Guia de Administração* e o *Guia de Instalação* para obter mais informações.

Ajuste dos componentes de tempo de execução

As alterações nos negócios no CA IdentityMinder são realizadas por meio de tarefas. Uma tarefa contém um ou mais eventos, que representam atividades que o CA IdentityMinder executa para concluir a tarefa. Por exemplo, a tarefa Criar usuário pode incluir CreateUserEvent e AddToGroupEvent.

O CA IdentityMinder inclui os seguintes componentes, que processam tarefas e eventos em tempo de execução:

- Bancos de dados do CA IdentityMinder, que oferecem suporte à funcionalidade do CA IdentityMinder
- Mensagens JMS, que são responsáveis pelo processamento de eventos

Ajuste dos bancos de dados do CA IdentityMinder

Ao executar tarefas, o CA IdentityMinder usa os seguintes bancos de dados:

- Persistência de tarefas

  Mantém informações sobre tarefas e eventos do CA IdentityMinder ao longo do tempo. Isso permite que o CA IdentityMinder restaure o último estado conhecido de eventos e tarefas no caso de uma falha do sistema.

  Observação: esse banco de dados tem impacto mais significativo sobre o desempenho do CA IdentityMinder, pois a tarefa e seus eventos são salvos e recuperados do banco de dados durante transições de estado.

- Auditoria

  Fornece um registro histórico de operações que ocorrem em um ambiente do CA IdentityMinder.

- Fluxo de trabalho

  Armazena definições de processo do fluxo de trabalho, tarefas, scripts e outros dados exigidos pelo Mecanismo de fluxo de trabalho.

- Geração de relatórios

  Armazena dados de instantâneo, que reflete o estado atual dos objetos no CA IdentityMinder no momento em que o instantâneo é gerado.

O CA IdentityMinder se comunica com cada banco de dados por meio de um pool de conexões JDBC. É possível criar e configurar um pool de conexões JDBC no servidor de aplicativos que hospeda o CA IdentityMinder. Ao configurar o pool de conexões JDBC, observe o seguinte:

- Considere a quantidade de tarefas simultâneas que será executada em um dado momento.
- Considere os outros componentes de tempo de execução ao configurar o tamanho do pool de conexões JDBC. Cada componente de tempo de execução funciona em conjunto com os outros componentes de tempo de execução.

  Observação: a CA recomenda definir o valor inicial do pool de conexões para 128.

- Para o banco de dados de persistência de tarefas, o número de conexões de banco de dados no pool deve permitir que cada tarefa em execução recupere e atualize os dados de tarefa e evento durante todo o tempo de vida útil da tarefa.
- O banco de dados de persistência de tarefas usa instruções preparadas. Não se esqueça de configurar o cache da instrução preparada para o banco de dados que você está usando para armazenar dados de persistência de tarefas.

  Observação: consulte a documentação do banco de dados que você está usando para persistência de tarefa de modo a obter informações sobre como configurar o cache da instrução preparada.

Configurações do JMS

Uma tarefa do CA IdentityMinder inclui eventos, ações que o CA IdentityMinder executa para concluir uma tarefa.

Durante o ciclo de vida de um evento, ele passa pelos seguintes estados:

- BEGIN
- APPROVED
- EXECUTING
- COMPLETED
- INVALID

Os eventos controlados pelo fluxo de trabalho também podem apresentar estes estados:

- PENDING
- REJECTED

O CA IdentityMinder usa mensagens JMS para controlar essas transições de estado.

Como as mensagens JMS orientam as transações de evento

O CA IdentityMinder usa mensagens JMS para orientar as transições de estado de um evento. O procedimento a seguir descreve as etapas envolvidas:

1. Um usuário envia uma tarefa.
2. A tarefa gera um ou mais eventos.
3. Quando um evento estiver pronto para processamento, o CA IdentityMinder definirá o estado do evento para BEGIN e o evento será mantido no banco de dados de persistência de tarefas.
4. O CA IdentityMinder cria uma mensagem JMS contendo a ID do evento e publica essa mensagem na Fila de mensagens de eventos.
5. Ao receber a mensagem, o JMS chama uma instância do Message Driven Bean do evento, que é uma implementação do Controlador de eventos.
6. O Controlador de eventos usa a ID do evento na mensagem para recuperar o evento do banco de dados de persistência de tarefas e executa as ações do estado atual do evento.
7. Após a conclusão desse estado, o evento é definido para o próximo estado, mantido no banco de dados de persistência de tarefas, e uma nova mensagem JMS é postada para processamento do próximo estado.

   Esse ciclo continuará até que o evento tenha concluído sua máquina de estado.

Mensagens JMS e desempenho

Para qualquer evento, há de três a cinco estados que exigem mensagens JMS para transição de estado:

- BEGIN
- PENDING (somente no controle de Fluxo de trabalho)
- APPROVED ou REJECTED
- EXECUTING
- COMPLETED ou INVALID

Para processar um único evento, as seguintes ações serão executadas:

- Três a cinco postagens na Fila de mensagens de eventos
- Três a cinco invocações do Message Driven Bean
- Seis a dez conexões com o banco de dados de persistência de tarefas (uma ação de leitura e uma ação de gravação por estado)

Essas ações podem afetar o tempo que o CA IdentityMinder leva para processar uma tarefa.

Para assegurar o melhor desempenho durante as transições de estado, ajuste os recursos JMS no servidor de aplicativos que hospeda o CA IdentityMinder para que ele se ajuste aos recursos JMS disponíveis.

Ajustando as configurações do JMS

Os seguintes parâmetros de ajuste JMS do servidor de aplicativos definem as conexões de fila e os pools de instância do Message Driven Bean.

- **Ajuste JMS do WebSphere**

  O WebSphere fornece aos Queue Connection Factories dois parâmetros que você pode configurar para melhorar o desempenho. Use o Console de administração do WebSphere para definir as seguintes propriedades:

  - Em Resources, localize os seguintes Queue Connection Factories: iam-im-neteQCF e iam-im-wpConnectionFactory.
  - Em cada um, edite as propriedades do pool de conexões para definir as conexões máximas para 128.

- **Ajuste do WebLogic**

  Nos servidores de aplicativos do WebLogic, os Queue Connection Factories obtêm segmentos de manipulação de conexão do Pool de segmentos JMS do servidor ou do pool de execuções padrão, dependendo do tamanho do Pool de segmentos JMS. Se o tamanho do Pool de segmentos JMS for 0, o WebLogic usará os segmentos no pool de execuções.

  É recomendável definir o número de segmentos do Pool de segmentos JMS para ser igual ao tamanho máximo do Pool de beans do Message Driven Bean de eventos do CA IdentityMinder, que é definido para 128 por padrão.

  Você pode usar o Console do servidor do WebLogic para definir o tamanho do Pool de segmentos JMS nas propriedades dos Serviços JMS para o domínio e servidor onde o CA IdentityMinder está instalado.

  O tamanho do pool do Message Driven Bean de eventos do CA IdentityMinder é definido pela modificação da configuração max-beans-in-free-pool no arquivo descritor no seguinte local:

  WebLogic_home\domain\applications\iam_im.ear\identityminder_ejb.jar\META-INF\weblogic-ejb-jar.xml

```
<weblogic-enterprise-bean>
        <ejb-name>SubscriberMessageEJB</ejb-name>
        <message-driven-descriptor>
            <pool>
                <max-beans-in-free-pool>128</max-beans-in-free-pool>
                <initial-beans-in-free-pool>16</initial-beans-in-free-pool>
            </pool>

<destination-jndi-name>com.netegrity.ims.msg.queue</destination-jndi-name>
        </message-driven-descriptor>
    </weblogic-enterprise-bean>
```

- **Ajuste do JBoss**

  No servidor de aplicativos do JBoss, os Queue Connection Factories obtêm segmentos de manipulação de conexões do alocador de sessão do Pool JMS padrão do servidor. Por padrão, o número máximo de segmentos é definido como 15.

  Aconselhamos definir esse valor para corresponder ao valor do tamanho máximo do Recipiente padrão do bean de mensagem.

O alocador da seção Pool de sessão JMS é definido no elemento MaximumSize do JMSContainerInvoker no seguinte arquivo:

base_do_jboss\server\default\conf\standardjboss.xml

```
<invoker-proxy-binding>
         <name>message-driven-bean</name>
         ….
         <proxy-factory-config>

<JMSProviderAdapterJNDI>DefaultJMSProvider</JMSProviderAdapterJNDI>

<ServerSessionPoolFactoryJNDI>StdJMSPool</ServerSessionPoolFactoryJNDI>
            <MaximumSize>128</MaximumSize>
            <MaxMessages>1</MaxMessages>
            ….
         </proxy-factory-config>
     </invoker-proxy-binding>
```

O tamanho do pool do Message Driven Bean de eventos do CA IdentityMinder é definido pela modificação do valor do tamanho máximo no seguinte arquivo descritor:

base_do_jboss\server\default\conf\standardjboss.xml

```
<container-configuration>
         <container-name>Standard Message Driven Bean</container-name>
         <call-logging>false</call-logging>

<invoker-proxy-binding-name>message-driven-bean</invoker-proxy-binding-name>
        ……
         <container-pool-conf>
            <MaximumSize>128</MaximumSize>
         </container-pool-conf>
   </container-configuration>
```

Ajustando o desempenho do JBoss 5

Em uma instalação padrão do JBoss 5, o verificador de implantação online do JBoss é executado a cada 5 segundos, que afeta o desempenho do JBoss. É possível desativar esse recurso, se ele não for necessário, ou alterar a frequência com que ele é executado.

Para desativar ou modificar a implantação online

1. Edite o hdscanner-jboss-beans.xml neste local:

   Único nó: *base_do_jboss*/server/default/deploy

   Cluster: *base_do_jboss*/server/all/deploy

2. Para desativar esse recurso, adicione a seguinte linha no bean HDScanner:
   `<attribute name="ScanEnabled">False</attribute>`

3. Para modificar a frequência de verificação, aumente o valor do atributo scanPeriod para acima de 5000 (milissegundos).

Observação: para obter mais detalhes, consulte este link: http://community.jboss.org/wiki/JBossASTuningSlimming.

Para corrigir erros de falta de memória

Você pode ver exceções de "Memória insuficiente" se o tamanho do heap Java for muito pequeno. É recomendável um tamanho inicial de 1024.

Capítulo 7: Criando um plano de recuperação de falhas

Esta seção contém os seguintes tópicos:

Perda de serviço a partir de uma falha

No caso de uma falha, os usuários podem perder o acesso aos serviços que são essenciais para suas tarefas. Como resultado, esses usuários não podem fornecer serviços a outros usuários.

A urgência para restaurar o acesso aos serviços depende do real uso do CA IdentityMinder. Em algumas organizações, os usuários exigem acesso ininterrupto aos serviços fornecidos pelo CA IdentityMinder, enquanto outros usuários exigem restauração do sistema em um dia. Em qualquer caso, é recomendável fazer preparações para proteger a sua implementação do CA IdentityMinder de um evento que resulte em perda completa ou parcial dos seus sistemas.

Ao configurar uma arquitetura redundante do CA IdentityMinder, você pode garantir que os serviços sejam altamente disponibilizados para os usuários. Quando um componente principal falha, o componente alternativo continua fornecendo o mesmo serviço. Além disso, você pode fazer backup rotineiro de sistemas e softwares essenciais, para que seja possível restaurar qualquer sistema ou dado que seja totalmente perdido.

Este documento fornece diretrizes gerais de planejamento para esses cenários. Aconselhamos que você use essas diretrizes para desenvolver procedimentos específicos de recuperação de falhas que atendam aos requisitos de sua organização.

Como planejar a recuperação de falhas

Para desenvolver um plano de recuperação de falhas eficiente, você se envolve nas fases a seguir, que são detalhadas neste capítulo.

✓	**Fase**
	1. Definir requisitos da recuperação de falhas (na página 103) De acordo com as suas necessidades organizacionais, identifique quais tipos de falhas prever e quão rapidamente você deverá restaurar os serviços.
	2. Desenvolver uma arquitetura redundante (na página 104) De acordo com os seus requisitos, desenvolva uma arquitetura com componentes redundantes em um local remoto.
	3. Desenvolver planos de backup (na página 106) Para proteger sua instalação, desenvolva planos para fazer o backup de componentes.
	4. Desenvolver procedimentos de restauração (na página 107) Desenvolva procedimentos para restaurar componentes perdidos.
	5. Documentar o plano de recuperação (na página 110) Documente os seus planos para a recuperação de uma falha do CA IdentityMinder.
	6. Testar o plano de recuperação (na página 111) Com base nos seus procedimentos de recuperação de falhas, verifique se é possível restabelecer sua implementação do CA IdentityMinder para o mesmo estado em que ele existia antes do evento.
	7. Fornecer treinamento de recuperação de falhas (na página 112) Conclua o processo verificando se as pessoas responsáveis por recuperar os sistemas de uma falha foram treinadas para isso.

Definir requisitos da recuperação de falhas

Veja a seguir algumas orientações gerais a serem consideradas na definição de requisitos de um plano de recuperação de falhas:

1. Monte uma equipe com os seguintes conhecimentos:
   - Conhecimento da arquitetura e dos sistemas que oferecem suporte ao CA IdentityMinder
   - Conhecimento de como fazer backup dos bancos de dados relacionais e repositórios de usuários LDAP usados pelo CA IdentityMinder
2. Identifique os possíveis cenários de falhas a serem recuperados, incluindo perda parcial ou completa de sistemas em um ou mais sites.
3. Liste os sistemas que imprescindivelmente precisam estar disponíveis para oferecer suporte à sua instalação.
4. Defina o downtime máximo aceitável para cada um desses sistemas.

   Por exemplo, os sistemas que oferecem suporte a um servidor alternativo podem ter um nível de prioridade mais baixo para restauração.

Desenvolver uma arquitetura redundante

Para se proteger contra a falha de um componente essencial, considere as seguintes ações protetoras usando componentes alternativos (servidores e diretórios) e bancos de dados redundantes em locais remotos.

Configure a redundância do CA IdentityMinder usando o *Guia de Instalação* .Inclua os seguintes componentes:

- Nós do servidor de aplicativos do CA IdentityMinder redundantes como parte de um cluster
- Um cluster de Servidores de políticas que ofereça tolerância a falhas (se você estiver usando o CA SiteMinder para proteger o CA IdentityMinder)
- Servidores de provisionamento alternativos, Diretórios de provisionamento e servidores de conectores. Se um componente principal for perdido, o sistema alternará para o componente alternativo.

Configure a redundância de bancos de dados incluindo o seguinte:

- Qualquer um dos bancos de dados de tempo de execução que façam parte do CA IdentityMinder, como o fluxo de trabalho ou banco de dados de auditoria.

  Consulte a documentação fornecida com o servidor ORACLE ou Microsoft SQL Server.

- O banco de dados Business Objects se estiver usando o Servidor de relatórios.

  Consulte a documentação do Business Objects Enterprise, Release 2 e Release 2 SP4 no site de documentação da SAP.

Servidores alternativos do CA IdentityMinder

O fornecimento de nós redundantes do Servidor de aplicativos do Servidor do CA IdentityMinder proporciona benefícios de escalabilidade e desempenho, bem como recuperação de falhas em caso de falha de servidores individuais. O método mais comum de fornecer tolerância a falhas a um servidor de aplicativos é criar um cluster. Os procedimentos para a criação do cluster são discutidos na seção de cluster do *Guia de Instalação*.

Observação: para o CA IdentityMinder r12.0 e releases superiores, um cluster de servidores de aplicativos é o único método válido para implementar uma implantação de vários nós. Os ambientes do CA IdentityMinder exigem a arquitetura de cluster J2EE padrão do setor, que usa as filas JMS para o backbone. Consequentemente, o único método válido para usar vários nós em uma configuração do CA IdentityMinder é um cluster de servidores de aplicativos.

Para obter mais detalhes sobre essa alteração, consulte TechDoc 545594.

Componentes alternativos de provisionamento

Vários componentes de provisionamento têm a opção de um componente alternativo para fornecer alta disponibilidade. O componente alternativo deve estar em um site remoto para atingir a máxima proteção.

Consulte o capítulo Provisionamento de alta disponibilidade do *Guia de Instalação* para obter os detalhes específicos da configuração de servidores e diretórios alternativos.

Diretórios de provisionamento de vários sites

É possível criar diretórios de provisionamento principal e alternativo com os diretórios alternativos em um local remoto. O CA Directory recomenda instalar três Diretórios de provisionamento, um principal e dois alternativos.

Servidores de provisionamento de vários sites

Para se proteger contra falha do Servidor de provisionamento principal, você pode configurar um Servidor de provisionamento alternativo. A diferença entre os Servidores de provisionamento principal e alternativo é que a instalação do servidor principal preenche as entradas do recipiente do Diretório de provisionamento. Além disso, a desinstalação de um servidor principal remove essas entradas. Com exceção da instalação e da desinstalação, os servidores principal e alternativo funcionam da mesma forma.

Servidores de conectores de vários sites

Para Java ou C++ Connector Server, é possível configurar vários servidores de conectores para servir o mesmo terminal ou tipo de terminal.

Para cada servidor de conectores configurado, você deverá configurar um servidor de conectores alternativo em um local remoto para tratar do mesmo terminal. Se o servidor de conectores falhar, o servidor alternativo gerenciará imediatamente a comunicação com os terminais.

Bancos de dados redundantes

Os softwares de banco de dados suportados, Microsoft SQL Server e Oracle, têm a capacidade de fornecer bancos de dados redundantes. Se o banco de dados principal falhar, o banco de dados redundante será disponibilizado imediatamente. O banco de dados redundante deve estar em um site remoto no caso de todo o site ser afetado.

Desenvolver planos de backup

Para se proteger contra a perda de algum ou todos os sistemas, use o armazenamento fora da organização para todos os dados de backup e uma programação de backup que atenda aos seus requisitos de downtime máximo. Os procedimentos de backup e restauração usam diferentes aplicativos, de forma que eles devem ser coordenados para recuperação do sistema do CA IdentityMinder como um todo.

Inclua os seguintes componentes em seus planos de backup:

Componente	**Descrição**	**Método de backup**
O repositório de usuários do CA IdentityMinder	Um diretório de usuários LDAP ou um banco de dados relacional que contém os registros de usuários do CA IdentityMinder	Consulte a documentação fornecida com o banco de dados ou o software LDAP.
Os bancos de dados do CA IdentityMinder	Os bancos de dados para Persistência de tarefas, Fluxo de trabalho, Auditoria, Repositório de objetos, Relatórios e Arquivamento de persistência de tarefas Fluxo de trabalho, Persistência de tarefas e Auditoria que têm a frequência mais alta de alterações e backups devem ser programados de acordo.	Consulte a documentação fornecida com o software de banco de dados.
Repositório de políticas do SiteMinder	Um diretório de usuários LDAP ou um banco de dados relacional com objetos do Servidor de políticas do SiteMinder, se você estiver usando o SiteMinder	Consulte a documentação fornecida com o banco de dados ou o software LDAP.
Diretório de provisionamento	Um diretório de usuário LDAP que contém os registros para usuários e objetos de provisionamento	Consulte a documentação do CA Directory.
Repositórios persistentes JMS do servidor de aplicativos	Os repositórios usados para manter as mensagens de processamento de Evento de tarefas do CA IdentityMinder	Consulte a documentação do servidor de aplicativos.
Bancos de dados de relatórios	Banco de dados de instantâneos Bancos de dados do Business Objects	Consulte a documentação fornecida com o software de banco de dados.
Relatórios personalizados	Relatórios personalizados e arquivos XML relacionados	Consulte a documentação do Business Objects Enterprise, Release 2 e Release 2 SP4 no site de documentação da SAP.

Inclua os seguintes componentes em seus planos de backup usando um programa de backup do sistema de arquivos:

Componente	Descrição
Componentes do servidor web	Configuração dos componentes do servidor web implantado, como plugins do Servidor de aplicativos e Agentes web do SiteMinder. Um front-end de Servidor web será exigido se você estiver usando balanceamento de carga ou se estiver usando o SiteMinder para proteger o acesso ao Console de usuário.
Arquivos de dados XML	Todos os arquivos de Diretório e Ambiente do CA IdentityMinder que são usados para criar, manter e arquivar objetos do Repositório de objetos do CA IdentityMinder.
Componentes de personalização do CA IdentityMinder	Os arquivos encontrados nas seguintes pastas iam_im.ear implantadas: ■ Config ■ User_console.war WEB-INF\web.xml
Scripts e programas	Scripts, programas, saídas de programa para TEWS
Componentes do Connector Xpress	Conectores personalizados Arquivos de projeto do Connector Xpress
Documentação de recuperação de falhas	Após criar sua própria documentação para recuperação de falhas, faça backup dela regularmente, caso as instruções mudem.

Desenvolver procedimentos de restauração

Os procedimentos de restauração dependem do método de backup. O processo de recuperação para um sistema que falhou depende das circunstâncias. No entanto, em muitos casos, a reinstalação do software é o método de restauração. Consulte o capítulo Provisionamento de alta disponibilidade do *Guia de Instalação* para obter detalhes.

Restaurar o repositório de usuários do CA IdentityMinder

Para restaurar o repositório de usuários do CA IdentityMinder, consulte a documentação fornecida com seu software LDAP ou banco de dados. Verifique se o repositório de dados do backup está intacto, incluindo o acesso a todos os repositórios de usuários.

Restaurar os bancos de dados do CA IdentityMinder

Para restaurar os bancos de dados do CA IdentityMinder, consulte a documentação fornecida com o seu banco de dados. Verifique se o repositório de dados do backup está intacto, incluindo o acesso a todos os bancos de dados.

Restaurar o Repositório de políticas do SiteMinder

Para restaurar o repositório de políticas do SiteMinder, consulte a documentação fornecida com seu software LDAP ou banco de dados. Verifique se o repositório de dados do backup está intacto, incluindo o acesso a todos os repositórios de usuários.

Restaurar o Servidor do CA IdentityMinder

Se você perder um nó do cluster de um servidor do CA IdentityMinder, execute as seguintes etapas:

1. Use o procedimento documentado padrão para adicionar um nó.

   Consulte o capítulo sobre instalação de cluster no *Guia de Instalação.*

2. Atualize a conexão com o Servidor de provisionamento.

   Consulte a seção sobre Provisionamento de tolerância a falhas no capítulo Alta disponibilidade do *Guia de Instalação* para obter detalhes.

Restaurar um diretório e servidor de provisionamento

É possível restaurar um Servidor de provisionamento perdido instalando um servidor alternativo. Se todos os sistemas falharem, restaure os dados perdidos durante a falha.

Use as seguintes etapas:

1. Copie os arquivos de esquema personalizado no diretório config\schema do CA Directory.
2. Instale o novo Diretório de provisionamento.

   Os repositórios de dados estarão vazios.
3. Restaure os dados a partir do local de backup.
4. Use o instalador do Servidor de provisionamento, fornecendo os detalhes do Diretório de provisionamento recentemente restaurado.

   As informações de domínio já devem estar presentes.
5. Restaure todos os arquivos de configuração e conectores personalizados do backup.

Observação: para obter mais detalhes, consulte a documentação do CA Directory.

Restaurar servidores de conectores

Se você perder um servidor de conectores, execute as seguintes etapas:

1. Use o instalador do Servidor de conectores para instalar um novo servidor de conectores

   Registre-o no Servidor de provisionamento durante a instalação.
2. Remova o registro do servidor de conectores perdido usando csfconfig ou o Connector Xpress.

Restaurar um servidor de relatórios

Se você perder o servidor de relatórios, consulte a documentação do Business Objects para ver os procedimentos que devem ser aplicados. No site de documentação da SAP, verifique a documentação do Business Objects Enterprise, Release 2 e Release 2 SP 4.

Restaurar tarefas administrativas

Se uma tarefa administrativa estava em andamento no momento da falha, ela poderá ser recuperada sob as seguintes condições:

- Qualquer tarefa administrativa que estava em um estado Pendente aguardando aprovações continuará disponível se os repositórios usados para manter essas informações de estado forem preservados. O repositório inclui o banco de dados de Persistência de tarefas, o armazenamento JMS que mantém as mensagens JMS de tarefas e eventos, bem como o banco de dados de Fluxo de trabalho.
- As tarefas no estado Em andamento (qualquer estado diferente de Pendente) estão sujeitas às condições adicionais.

  Uma tarefa nesse estado exige a publicação de uma nova Mensagem JMS na Fila de mensagens de eventos do CA IdentityMinder para continuar sendo processada. As interrupções que ocorrem antes que esse evento seja postado na fila impedem a tarefa de continuar na recuperação.

  Nesse caso, há duas opções para recuperar a tarefa:

  - Se a tarefa estiver presente na tarefa Exibir tarefas enviadas no estado de falha, vá para a página de detalhes da tarefa e use a opção Resubmit Task para reenviar a tarefa.
  - Envie uma nova tarefa com as mesmas alterações.

Documentar o plano de recuperação

Com base nas diretrizes deste capítulo, aconselhamos que você desenvolva a documentação de recuperação de falhas específica que se aplique à sua organização.

Considere a seguinte abordagem:

1. Identifique os nomes e os locais de sistemas em sua arquitetura e os componentes alternativos para cada sistema.

   Para cada sistema, liste o software instalado, como o JDK específico instalado, a release de correção de um servidor de aplicativos e a quantidade de memória instalada. Esses detalhes são necessários para qualquer sistema que precise ser totalmente recriado.

2. Escreva procedimentos para recuperar cada componente ou para recriar um sistema completo, se necessário.
3. Identifique um método de localização ou redefinição de nomes de usuário e senhas para sistemas e interfaces de usuário do CA IdentityMinder, caso eles sejam conhecidos apenas por uma ou duas pessoas.
4. Proteja sua documentação de recuperação de falhas contra perda criando uma cópia de backup que você armazena em um local fora da instalação.

Testar o plano de recuperação

Para ajudar a garantir uma recuperação bem-sucedida após uma falha, você pode programar uma falha simulada, em que determinados sistemas tornam-se indisponíveis. Considere os seguintes testes, que são descritos nas seções a seguir.

1. Teste o processo de tolerância a falhas.
2. Teste a restauração dos sistemas.

Testar o processo de tolerância a falhas

Todos os servidores ou diretórios devem ter um servidor ou diretório alternativo em um site remoto, que inclua estes componentes:

- Servidor do CA IdentityMinder
- Servidor de provisionamento
- Diretórios de provisionamento
- C++ e Java Connector Servers
- Servidor de relatórios
- Servidor de políticas

Interrompa manualmente cada componente e verifique se todas as operações continuam funcionando, usando o componente alternativo. Por exemplo, você pode executar o teste a seguir do Servidor de provisionamento:

1. Em um sistema com o Servidor de provisionamento principal, interrompa os serviços do Serviço de provisionamento na caixa de diálogo Serviços do Windows.

   O Servidor de provisionamento principal é interrompido.

2. No Console de usuário, execute as seguintes ações:

   a. Atribua uma Função de provisionamento a um usuário.

   b. Verifique se as contas de terminal foram criadas para esse usuário.

      As contas que estão sendo criadas dependem do Servidor de Provisionamento alternativo que está manipulando a comunicação com o servidor do CA IdentityMinder.

Esse procedimento é o exemplo de um teste. Para cada componente que você interrompe, desenvolva testes semelhantes para verificar se o componente alternativo está em uso.

Testar os procedimentos de restauração

De acordo com sua documentação de recuperação de falhas, faça um teste de cada componente essencial para verificar se é possível restaurar o sistema perdido.

Fornecer treinamento de recuperação de falhas

Se você acredita que os procedimentos de recuperação são confiáveis, ajude a garantir que as pessoas que devem implementar a recuperação estejam aptas a fazê-lo. No entanto, sua organização pode exigir outras etapas. Veja a seguir algumas diretrizes gerais:

1. Publique o local da documentação de recuperação.
2. Execute uma simulação do treinamento.
3. Incorpore comentários no final do treinamento para ajudar a garantir que os procedimentos de recuperação de falhas sejam suficientes.

Observação: você também pode optar por usar o treinamento como uma oportunidade para atribuir coordenadores de recuperação, incluindo uma pessoa como o coordenador de recuperação e uma segunda pessoa como um coordenador alternativo. Essas pessoas devem ser instruídas a atender em um local documentado para dar início ao plano de recuperação de falhas.

Índice remissivo

A

B

C

D

E

F

G

I

L

M

O

P

R

S

T